The PCLinuxOS magazine
Volume 218
March, 2025

Happy St. Patrick's Day

Inside This Issue...

The PCLinuxOS magazine

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

Staff:

YouCanToo David Pardue

Contributors:

Ramchu kalwisti

David Marshall

From The Chief Editor's Desk

You might have noticed a new column in last month's issue of The PCLinuxOS Magazine. It's called **Wiki Pick**. This new column will feature a helpful article lifted straight from the pages of the PCLinuxOS Knowlegebase Wiki. We plan to make it a monthly feature.

There are multiple facets to the decision to introduce a new monthly column. One reason is to try to keep things fresh and interesting, and to provide things that we think that the PCLinuxOS community will like/use/enjoy. That these are helpful articles is a great benefit, as well.

Another reason is to help draw attention to the presence and existence of our newly restored Wiki. I personally know that CoreLite and The CrankyZombie worked very hard to restore the Wiki that was lost almost two years ago when the server it resides on was struck by ransomware scumbags. Having gone for nearly two years without a dedicated PCLinuxOS Wiki, the "habit" of visiting and using the Wiki has most probably been lost.

Ryan and dad showing off Ryan's completed arrow for his Cub Scout Arrow of Light ceremony. Ryan crosses over from the Cub Scout pack to the Scout Troop on March 1, 2025.

Our PCLinuxOS Knowledgebase Wiki, like virtually every other Wiki out there, is a community-supported and community-driven site to give all PCLinuxOS users a place to turn to for help and assistance. Sure, we have the forum, and for many users, the forum will continue to be their place to turn to for help and assistance. But the Wiki provides tried-and-true help and instructions for all sorts of topics, all without having to wait for someone to respond in the forum.

The forum and the Wiki are very different and separate entities. While the forum can also provide that help and assistance, it also provides a place for PCLinuxOS users to socialize and interact with other PCLinuxOS users. The Wiki, on the other hand, provides written

documentation and step-by-step "how-to's" without the banter and interaction. Most likely, when something has gone wrong, or if you're just looking for information on how to do something, you might not be "in the mood" for socializing.

Since ~~most~~ all wikis are user supported, the PCLinuxOS Knowledgebase Wiki cannot exist and thrive without user input. This is, literally, YOUR wiki! To be as useful as it can be, it requires users to contribute their specific knowledge so it can be shared with other users. If you have a solution for a problem or issue, you need to share it on the Wiki so that others having similar problems or issues can benefit from your having already resolved that problem or issue. And, no problem or issue is too small to be included in the PCLinuxOS Knowledgebase Wiki.

The Wiki is a great vehicle for users helping other users. Through the Wiki, we show the world that there is unity and caring among PCLinuxOS users. If users of other Linux distros benefit from information shared in the Wiki, that's a bonus. When/if those users are ever in search for a new distro (most of you know that Linux users are often prone to "distro hopping" … the "grass is always greener…"), they are likely to remember their positive experience by finding a solution to their problem or issue, and may help attract new users to PCLinuxOS. For those of us who have been around here for a while and "found our Linux home," we always welcome new users, who bring new ideas and new skills to our community.

****

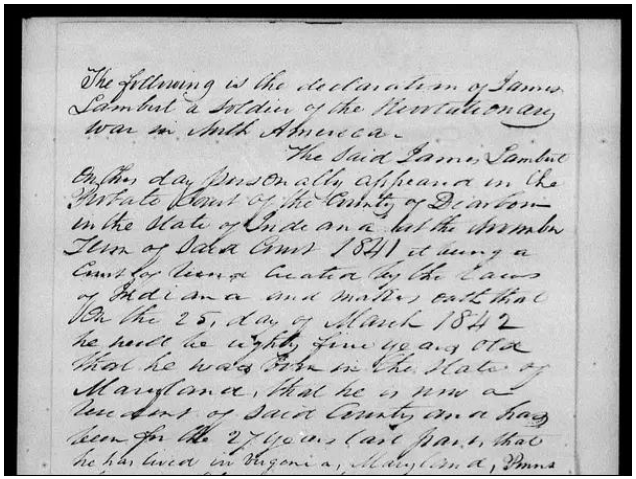
This month's cover celebrates St. Patrick's Day, and honors our Irish friends. Many immigrants came to the U.S. from Ireland, and St. Patrick's Day celebrates their contribution to life here. This month's cover image is a composite of the flag of Ireland, with a cute little Unicorn dressed out in an Irish motif. The flag image is from Wikimedia Commons, while the Unicorn image is from Pixabay artist Lynda Smith.

****

Until next month, I bid you peace, happiness, serenity, prosperity, and continued good health. Be careful out there. Around where I live, five maladies are circulating with fury: RSV, Influenza, Covid, Norovirus, and Mycoplasma pneumoniae (the bacterium most commonly associated with what lay people call "walking pneumonia").

ICYMI: Security Vulnerabilities Found In Multiple Tunneling Protocols

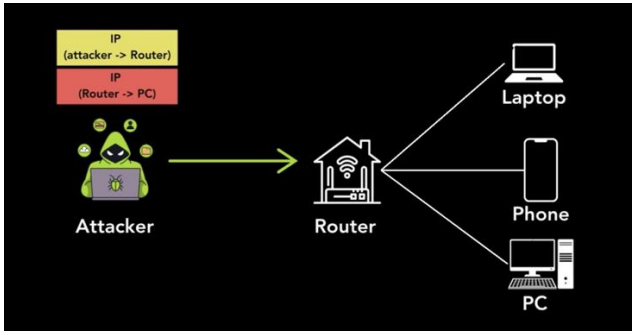
by Paul Arnote (parnote)



Can you read this cursive handwriting? The National Archives wants your help, according to an article from Smithsonian Magazine. Anyone with an internet connection can volunteer to transcribe historical documents and help make the archives' digital catalog more accessible. The National Archives is brimming with historical documents written in cursive, including some that date back more than 200 years. But these texts can be difficult to read and understand— particularly for Americans who never learned cursive in school. That's why the National Archives is looking for volunteers who can help transcribe and organize its many handwritten records: The goal of the Citizen Archivist program is to help "unlock history" by making digital documents more accessible, according to the project's website.

The phishing-as-a-service kit from Sneaky Log creates fake authentication pages to farm account information, including two-factor security codes, according to an article from TechRepublic. Security researchers at French firm Sekoia detected a new phishing-as-a-service kit targeting Microsoft 365 accounts in December 2024, the company announced on Jan. 16. The kit, called Sneaky 2FA, was distributed through Telegram by the threat actor service Sneaky Log. It is associated with about 100 domains and has been active since at least October 2024. Sneaky 2FA is an adversary-in-the-middle attack, meaning it intercepts information sent between two devices: in this case, a device with Microsoft 365 and a phishing server. Sneaky 2FA falls under the class of business email compromise attacks.

From the "here we go again" department, the Windows 11 24H2 patch breaks audio, Bluetooth, webcams, and more, continuing the trend from last year, according to an article from PCWorld. The first Windows 11 24H2 patch of 2025 is causing all sorts of problems. Update KB5050009, the first patch of the year for Windows 11, released two weeks ago on January 15. However, instead of fixing and improving the problematic 24H2 version of Windows 11 (which is now mandatory), this update once again brings with it a number of problems. As reported by Windows Latest, users are encountering various errors with sound output, Bluetooth connections, and more.



New research has uncovered security vulnerabilities in multiple tunneling protocols that could allow attackers to perform a wide range of attacks, according to an article from The Hacker News. "Internet hosts that accept tunneling packets without verifying the sender's identity can be hijacked to perform anonymous attacks and provide access to their networks," Top10VPN said in a study, as part of a collaboration with KU Leuven professor and researcher Mathy Vanhoef. As many as 4.2 million hosts have been found susceptible to the attacks, including VPN servers, ISP home routers, core internet routers, mobile network gateways, and content delivery network (CDN) nodes. China, France, Japan, the U.S., and Brazil top the list of the most affected countries. Successful exploitation of the shortcomings could permit an adversary to abuse a susceptible system as one-way proxies, as well as conduct denial-of-service (DoS) attacks.

Could the Carrington Event happen again? It happened in 1859. Today, it would be

catastrophic, according to an article from Popular Science. On a hot and humid Florida night in late August 1859, the sky suddenly lit up. But it was not from fireflies or a fireswamp. Instead, it was the Northern Lights–or aurora borealis. The aurora is usually seen in far more northern latitudes, but it had somehow reached the subtropics and danced across the night sky. Reports of the aurora came in from as far south as Central America and some in the Rocky Mountains even believed it was morning because the sky was so bright. “In a world that is now so dependent on electricity and electronics, a similar event has the potential to cause widespread disruptions and damage to the electronics aboard Earth-orbiting satellites, ground-based electronics, and the power grid,” said Alex Gianninas, an astrophysicist at Connecticut College.

Security researchers from Georgia Institute of Technology and Ruhr University Bochum discovered two side-channel vulnerabilities in devices with Apple name-brand chips from 2021 or later that could expose sensitive information to attackers, according to an article from TechRepublic. Specifically, the vulnerabilities known as SLAP and FLOP skim credit card information, locations, and other personal data. Data can be gathered from sites like iCloud Calendar, Google Maps, and Proton Mail via Safari and Chrome. As of late January, Apple is aware of the vulnerabilities. “Based on our analysis, we do not believe this issue poses an immediate risk to our users,” an Apple representative told ArsTechnica. According to the researchers, Apple plans to release a patch at an undisclosed time. The researchers have not found evidence of threat actors using these vulnerabilities.

Image by sutulo from Pixabay

A new study has found that US communities exposed to drinking water contaminated with 'forever chemicals' have up to 33 percent higher rates of certain cancers, according to an article from ScienceAlert. Scientists have good reason to believe a number of compounds referred to as PFAS (per- and poly-fluoroalkyl substances) are linked to cancer: they've already been implicated in kidney, breast, and testicular cancer, with at least one of the chemicals, PFOA, labeled as a carcinogen by the International Agency for Research on Cancer. These chemicals were first used in consumer and industrial products in the 1940s, and though many have been replaced, PFAS unfortunately have a lasting legacy thanks to their remarkable thermal and chemical stability. They're in our raincoats and upholstery, food packages, non-stick pots and pans, and fire-fighting foams. As these things disintegrate and become peppered throughout our environments, they've wound up in our food, our drinking water, and our bodies, too.

According to an article from Lifehacker, **Comcast just gave six cities an early look at lag-free internet**. L4S is an open-source standard that aims to significantly reduce latency online, and Comcast is among the first to allow customers access to it. If you live in Atlanta, Chicago, Philadelphia, San Francisco, Colorado Springs, or Rockville (Maryland), Comcast might have just given you a sneak peak at the internet of the future. In collaboration with Apple, Meta, Nvidia, and Valve, the service provider is currently rolling out its implementation of a new open standard called “L4S,” which seeks to drastically reduce how much lag impacts its customers, and make gaming and video calls much smoother.

Facebook is banning posts that mention various Linux-related topics, sites, or groups, according to an article from Tom’s Hardware. Some users may also see their accounts locked or limited when posting Linux topics. Major open-source operating system news, reviews, and discussion site DistroWatch is at the center of the controversy, as it seems to be the first to have noticed that Facebook's Community Standards had blackballed it. A post on the site claims, "Facebook's internal policy makers decided that Linux is malware and labeled groups associated with Linux as being 'cybersecurity threats.' We tried to post some blurb about distrowatch.com on Facebook and can confirm that it was barred with a message citing Community Standards. DistroWatch says that the Facebook ban took effect on January 19. Readers have reported difficulty posting links to the site on this social media platform. Moreover, some have told DistroWatch that their Facebook

accounts have been locked or limited after sharing posts mentioning Linux topics. Facebook's overzealous ban on some Linux topics in the name of Community Standards and its protection of its users from threats come with a large ladle full of irony. "Facebook runs much of its infrastructure on Linux," DistroWatch points out, "and often posts job ads looking for Linux developers." *(**Editor's Note**: it has been reported in multiple media outlets that Facebook has relaxed their stance on Linux posts, and has blamed the problem on overzealous settings in the software enforcing the "Community Standards.")*

Image by PDPhotos from Pixabay

Here's a nice example of AI producing inaccurate information, or just AI running amok. **Google just debuted a series of Super Bowl ads showing how small businesses use Gemini AI across all 50 states**, but the cheese lovers out there might notice something a little off about its Wisconsin one, according to an article from The Verge. As spotted by @natejhake on X, the ad shows Gemini AI generating text that says Gouda accounts for "50 to 60 percent of the world's cheese consumption" — a stat that isn't quite accurate. The cheese is undoubtedly popular in Europe, but the same can't be said for the rest of the world. "While Gouda is likely the most common single variety in world trade, it is almost assuredly not the most widely consumed," Andrew Novakovic, E.V. Baker Professor of Agricultural Economics Emeritus at Cornell University, tells The Verge.

Chinese astronauts have created rocket fuel in space using "artificial photosynthesis," according to an article from Futurism.com. Could this be the key for generating breathable air on the Moon? Chinese astronauts claim to have created rocket fuel on board the country's Tiangong space station using a new process dubbed "artificial photosynthesis." As the South China Morning Post reports, space travelers from the current Shenzhou-19 mission produced the necessary ingredients of rocket fuel, as well as oxygen, another useful resource in space. The team used semiconductor catalysts to turn carbon dioxide and water into oxygen and ethylene, a hydrocarbon commonly used to produce spacecraft propellants, according to the SCMP.

A groundbreaking discovery by researchers at the University of California, **Los Angeles (UCLA) has challenged a long-standing rule in organic chemistry known as Bredt's Rule**, according to an article from Glass Almanac. Established nearly a century ago, this rule stated that certain types of specific organic molecules could not be synthesized due to their instability. UCLA's team's findings open the door to new molecular structures that were previously deemed unattainable, potentially revolutionizing fields such as pharmaceutical research.

Google blocked 2.3 million Android app submissions to the Play Store in 2024 due to violations of its policies that made them potentially risky for users, according to an article from BleepingComputer. In addition, 158,000 developer accounts were banned for attempting to publish harmful apps like malware and spyware on Android's official app store. In comparison, Google blocked 2,280,000 risky apps in 2023 and 1,500,000 apps in 2022, while the figures for blocked Play developer accounts were 333,000 and 173,000, respectively. The

larger number of blocked apps in 2024 is partly attributed to AI assisting human reviews, which was used in 92% of the violating cases. "Today, over 92% of our human reviews for harmful apps are AI-assisted, allowing us to take quicker and more accurate action to help prevent harmful apps from becoming available on Google Play," explained Google.

A backdoor has been found in two healthcare patient monitors, linked to an IP in China, according to an article from Bleeping Computer. The US Cybersecurity and Infrastructure Security Agency (CISA) is warning that Contec CMS8000 devices, a widely used healthcare patient monitoring device, include a backdoor that quietly sends patient data to a remote IP address and downloads and executes files on the device. Contec is a China-based company that specializes in healthcare technology, offering a range of medical devices including patient monitoring systems, diagnostic equipment, and laboratory instruments. CISA learned of the malicious behavior from an external researcher who disclosed the vulnerability to the agency. When CISA tested three Contec CMS8000 firmware packages, the researchers discovered anomalous network traffic to a hard-coded external IP address, which is not associated with the company but rather a university.

Scientists have identified the Camp Hill virus, a henipavirus, in shrews in Alabama, marking its first detection in North America, according to an article from SciTechDaily. Researchers at the University of Queensland have discovered the first henipavirus detected in North America. Dr. Rhys Parry from the School of Chemistry and Molecular Biosciences confirmed the presence of Camp Hill virus in shrews in Alabama, USA. “Henipaviruses have caused serious disease and death in people and animals in other regions,” Dr Parry said. “One of the most dangerous is the Hendra virus, which was first detected in Brisbane, Australia, and has a fatality rate of 70 percent. Another example is Nipah virus which has recorded fatality rates between 40 and 75 per cent in outbreaks in Southeast Asia, including in Malaysia and Bangladesh. The discovery of a henipavirus in North America is highly significant, as it suggests these viruses may be more globally distributed than previously thought.”

Image by VIKAS SINGH CHHONKER from Pixabay

It should be as easy to cancel a service as it is to subscribe to it, and at long last, it's about to be, according to an article from Lifehacker. For anyone who's ever found themselves trapped in an endless maze of customer service calls trying to cancel a subscription — especially when the company doesn't want you to — relief is finally on the way. The Federal Trade Commission (FTC) has introduced a new rule that will require companies to make canceling subscriptions as simple as signing up for them. Under the new FTC regulation, if you can sign up for a service online with a single click, companies must provide an equally straightforward cancellation process. No more lengthy phone calls, buried cancellation links, or complicated multi-step procedures. This consumer-friendly rule aims to eliminate what's known as "dark patterns," aka deceptive design practices that make it unnecessarily difficult to cancel subscriptions.

Google has been feverishly integrating AI into as many of its products as it can, despite all of AI’s failings (at this point). Granted, AI is literally in its infancy, but dealing with the tantrums, fits, and inaccuracy of the toddler known as AI can become trying, at the very least. **Well, there is one way to make sure that**

AI isn't used for your Google searches: swear at it. Literally. If the first word in your search is **fsck** (hint: replace the second letter with a vowel that drastically changes its meaning), you will get Google's non-AI search results, according to an article from Lifehacker. Remarkably (and yet unsurprisingly), the standard search results are almost identical to the "AI-enhanced" search. Who'da thunk it?

I'm a Firefox user, and I have been since Firefox was first released. It is my go-to choice for a web browser. BUT … every six months or so, the Firefox team at Mozilla goes in and messes things up for a large percentage of users. See, I (and many other Firefox users) abhor having my tab bar above my toolbar. So that starts a mad twice-a-year scramble to search for the proper and updated CSS code to change things back to how they should be (with the tabs below the toolbar and bookmarks bar). The endless pursuit of finding the proper code to move my "tabs on bottom" is getting old and tiring. Always before, I went to MrOtherGuy's GitHub page (firefox-csshacks) and downloaded the updated CSS file to move my tab bar back to the bottom (not the bottom of the window, but below the toolbar and bookmarks bar). Well, that dog-chasing-his-tail dance may be finally over. From the AskVG website, he has **come up with an infinitely easier custom CSS file that just may survive the Mozilla devs endless and unyielding attempts to force us into submission**. Don't worry … he has full, easy-to-follow, step-by-step instructions on how to make the change. (**Tip**: Midori, Xfce's official browser, is built on the Firefox web engine, and they include a simple radio button to facilitate moving your tab bar to the bottom of the other "bars" under Settings > Design > Tab Bar. It feels and behaves just like Firefox, and is lighter weight than Firefox.)

A Chinese hacking group is hijacking the SSH daemon on network appliances by injecting malware into the process for persistent access and covert operations, according to an article from Bleeping Computer. The newly identified attack suite has been used in attacks since mid-November 2024, attributed to the Chinese Evasive Panda, aka DaggerFly, cyber-espionage group. As per the findings of Fortinet's Fortiguard researchers, the attack suite is named "ELF/Sshdinjector.A!tr" and consists of a collection of malware injected into the SSH daemon to perform a broad range of actions. Fortiguard says ELF/Sshdinjector.A!tr was used in attacks against network appliances, but although it has been documented previously, no analytical reports exist on how it works. The Evasive Panda threat actors have been active since 2012 and were recently exposed for conducting attacks deploying a novel macOS backdoor, carrying out supply chain attacks via ISPs in Asia, and collecting intelligence from U.S. organizations in a four-month-long operation.

In September 2023, a round, black capsule the size of a mini fridge fell from the sky, parachuting into a Department of Defense training site in the arid Utah desert. The modest container was holding samples collected from Bennu, a diamond-shaped asteroid billions of miles away, and had been traveling through the dark corridors of space for years, according to an article from SF Gate. After it was airlifted to a hangar via helicopter, researchers connected the capsule to a steady stream of nitrogen to protect its otherworldly cargo from outside contamination. **Slowly, they began to study it under a microscope — and, to their surprise,**

they discovered that this ancient, extraterrestrial object has a similar mineral makeup to one of California's most unusual lakes. According to a January 2025 study published in Nature, the Bennu asteroid samples contain six of the same minerals observed at San Bernardino County's Searles Lake: calcite, dolomite, gaylussite/pirssonite, thénardite, trona and halite.

Just when you thought things couldn't get worse for Boeing, here comes more bad news for the embattled aerospace company. Nearly five months after an uncrewed Starliner undocked from the International Space Station (ISS), **Boeing announced that it lost an additional half a billion dollars from its troubled spacecraft as the fate of its contract with NASA remains unclear**, according to an article from Gizmodo. In its filing with the Securities and Exchange Commission on Tuesday, Boeing reported a total of $523 million in losses from the Starliner Commercial Crew Program in 2024. That brings the total amount of losses from the ill-fated program to a whopping $2 billion in cost overruns. Boeing cited "highly complex designs and technical challenges," as well as "schedule delays and cost impacts," that increased the cost estimates for its programs. Under its $4.2 billion contract with NASA, Boeing retains full ownership of the Starliner spacecraft while NASA acts as a customer. Following Starliner's failed crewed test to the ISS, the company reported $250 million in losses for the third quarter, covering cost overruns out of its own pocket. That's on top of the $125 million it lost in the second quarter. Boeing had forewarned that more losses were coming during the fourth quarter of 2024, and it turned out to be the heftiest bill of the entire year.

Ransomware payments took an unexpected plunge in 2024, dropping 35% to approximately $813.55 million — despite payouts surpassing $1 billion for the first time in 2023, according to an article from TechRepublic. The decline was largely driven by a series of successful law enforcement takedowns and improved cyber hygiene, which enabled more victims to refuse payment, according to blockchain platform Chainalysis. The drop came as a surprise, considering the upward trend seen earlier in the year. In fact, ransomware actors extorted 2.38% more in the first half of 2024 compared to the same period in 2023, suggesting that payments would continue to rise. However, this momentum was short-lived, as payment activity plummeted by approximately 34.9% in the second half of the year. According to Chainalysis, Akira was the only one of the top 10 most prolific ransomware groups from the first half of 2024 to have increased its efforts in the second half. Additionally, as the year progressed, fewer exceptionally large payouts were made compared to the record-breaking $75 million payment to Dark Angels in early 2024.

On Jan. 29, U.S.-based Wiz Research announced it responsibly disclosed a DeepSeek database previously open to the public, exposing chat logs and other sensitive information, according to an article from TechRepublic. DeepSeek locked down the database, but the discovery highlights possible risks with generative AI models, particularly international projects. DeepSeek shook up the tech industry over the last week as the Chinese company's AI models rivaled American generative AI leaders. In particular, DeepSeek's R1 competes with OpenAI o1 on some benchmarks.

Pure Lithium

While certain tips and tricks can speed up the process and extend your phone battery's life, there's nothing you can do about the limitations of the lithium-ion batteries in your devices. They all eventually stop holding a charge, which means they constantly need replacing. There is, however, new hope for a breakthrough in battery technology, according to an article from Vox. **A Boston-based startup called Pure Lithium recently announced a breakthrough with its lithium metal batteries.** While the lithium-ion batteries in your phone start to degrade significantly after a few hundred cycles of charging and discharging, these lithium metal

batteries, which use pure lithium rather than a lithium compound, can last over 2,000 cycles without significant damage degradation, an ongoing test shows. Plus, the lithium metal batteries can store twice as much energy and weigh half as much as conventional lithium-ion batteries.

While it may be convenient, storing your passwords in Google Chrome's built-in password manager may not be the best security decision you've ever made, according to an article from TechRepublic. Considering the endless roll of Chrome vulnerabilities (many of which get covered virtually every month, right here in this monthly column), I couldn't agree more. The article will give you guidance on how to locate and remove your passwords from Chrome's password manager, and to replace it with something a LOT more robust. One of those solutions touted in the article is Bitwarden, which is in the PCLinuxOS repository.

A massive crack is widening across Africa, hinting at a transformation deep beneath the surface, according to an article from Daily Galaxy. Tectonic forces are reshaping the land faster than expected, with signs of an emerging ocean. Scientists are closely monitoring the shift, uncovering clues about what's unfolding beneath our feet. The continent's future is changing, and the implications could be enormous. Recent studies suggest this process, once thought to span tens of millions of years, could unfold in as little as a million years — maybe even sooner.

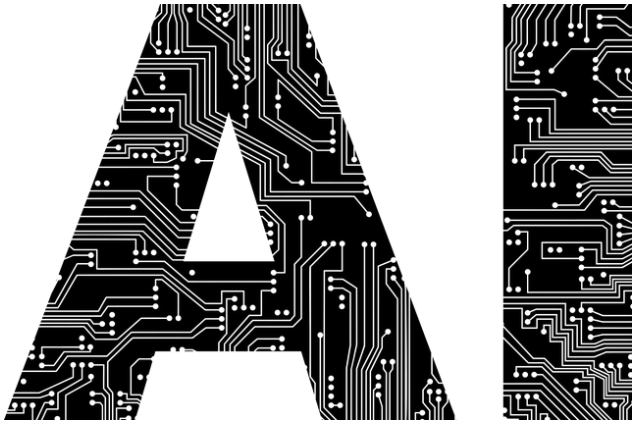


Image by Gordon Johnson from Pixabay

If you are even a little skeptical or concerned about AI and AI "overreach," you're gonna love this next little bit. **It turns out that getting your news from robots playing telephone with actual sources might not be the best idea**, according to an article from Lifehacker. In a BBC study (PDF) of OpenAI, Google Gemini, Microsoft Copilot, and Perplexity's news prowess, the news organization found that "51% of all AI answers" about news topics had "significant issues of some form." The study involved asking each bot to answer 100 questions about the news, using BBC sources when available, with their answers then being rated by "journalists who were relevant experts in the subject of the article."

OK. We don't usually promote the onslaught of "the sky is falling"/"the Earth is getting hit by an asteroid" articles. My "news" feed in Google News is littered with them — daily (I don't usually read them … but I've clicked on a rare one a long time ago, so Google thinks I want to see them all the time). But this one may be a little different. According to an article from Science Alert, at the end of 2024, **astronomers detected an asteroid in the night sky.** It was given the designation Y, since it was discovered in the last half of December, and R4 since it was the 117th rock to be found in the last couple of weeks of December, and since it was discovered in 2024, it was assigned the name 2024 YR4. As of this writing, **it now has a 2.3% chance of striking Earth on December 22, 2032.** While you might think this resembles the plot of Don't Look Up, none of this is too unusual. The 2.3% odds aren't simply the chances of a die roll. What it means is that when astronomers run 1,000 orbital simulations based on the data we have, 23 of them impact Earth. A later article from the New York Times places the chance of 2024 YR4 hitting Earth in 2032 at 3.1%. An even LATER article from the New York Times says, "The odds that the space rock, 2024 YR4, will smash into our planet in 2032 have dropped to nearly zero, leading astronomers to conclude that we are no longer in danger."

According to an article from TechRepublic, **the U.K.'s office of the Home Secretary has allegedly asked Apple to provide a backdoor into any material any user has uploaded to iCloud worldwide**, The Washington Post reported on Feb. 7. Anonymous sources provided The Washington Post the information and expressed concerns about tech companies being leveraged for government surveillance. As reported by The Washington Post, Apple received notice of a possible request in March 2024, but the official request occurred in January 2025. Apple has not commented.

However, in March, the company provided a statement to Parliament on the occasion of receiving notice of a potential request, saying "There is no reason why the U.K. [government] should have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption."

Image by Gerd Altmann from Pixabay

Microsoft's February 2025 Patch Tuesday, was on February 11, and includes security updates for 55 flaws, including four zero-day vulnerabilities, with two actively exploited in attacks, according to an article from Bleeping Computer. This Patch Tuesday also fixes three "Critical" vulnerabilities, all remote code execution vulnerabilities. The number of bugs in each vulnerability category is listed here: 19 Elevation of Privilege Vulnerabilities, 2 Security Feature Bypass Vulnerabilities, 22 Remote Code Execution Vulnerabilities, 1 Information Disclosure Vulnerabilities, 9 Denial of Service Vulnerabilities, 3 Spoofing Vulnerabilities, and a partridge in a pear tree. The numbers do not include a critical Microsoft Dynamics 365 Sales elevation of privileges flaw and 10 Microsoft Edge vulnerabilities fixed on February 6.

Western Digital acquired SanDisk back in 2015 for $16 billion. Just shy of 10 years later, that marriage is coming to an end. **Western Digital (WD) and SanDisk are slated to separate into two independent companies (again) shortly**, according to an article from PetaPixel. The plan was announced as far back as 2023 but has been delayed, stretching out the process until 2025. WD announced it planned to split its HDD and flash memory businesses on October 30, 2023, which would create two independent, public companies. Last March, WD said it was "on track" to spin off the Flash memory business from the core WD business sometime in the second half of 2024. That didn't happen, likely because the separation is what WD describes as "complex." Support for both businesses has divorced and WD moved all of its support for flash memory products — including its WD Black SSDs as well as HGST and G-Technology SSDs — to SanDisk's website last November.

In other news from Sandisk… According to another article from PetaPixel, after a series of lousy hardware faults, SanDisk's name turned to mud. **More than a year later, the company hopes to make people forget with a fresh new logo.** As spotted by Creative Bloq, the new Sandisk logo is making waves, although not entirely for the right reasons. As Joe Foley observes, Sandisk's — yes, it's "Sandisk" now, not "SanDisk" — rebrand follows recent design trends by removing bits of typeface from the wordmark. Kia did it, and so too did Nokia. In Sandisk's words, though, there's more to it than simple trend-chasing — the company is trying to rebrand, relaunch, and, reading between the lines, help people forget about recent controversies.

Image by Kohji Asakawa from Pixabay

It's hard to escape AI these days. Apple just made Apple Intelligence opt out, and Google Workspace users are now seeing big, hard-to-dismiss Gemini buttons all over their apps. The world's biggest tech companies are doing their best to sell you on a generative AI future, but even when you can't turn AI off, there are steps you can take to fight back. Even outside of Workspace, Google is one of the most egregious AI pushers around. The company has tried to push its Gemini AI in almost all of its properties, even though it's shown inaccurate search results recommending everything from eating rocks to adding glue to pizza. Even if you have no interest in AI search results, you'll still be forced to see elements of Google's Gemini all over Gmail and its other web apps. If that gets your goat, no worries—you can use

Hide Gemini, **a Chrome extension that hides Google Gemini elements from various Google sites** — to pretend you live in the good older days of 2020.

As kids become older, they become savvier at working their way around the parental controls on their devices. Time limits are tampered with, and apps I thought were deleted from our iPad suddenly reappear. While they're not yet accessing dangerous content, it's only a matter of time until they do. **Most routers have parental controls included, allowing concerned parents to put controls over all the devices that rely on wifi to ensure they don't go to dangerous sites.** If you're looking for a way to control what your family can access on the internet and for how long, this Lifehacker article has instructions for the three of the most popular router brands: TPLink, NetGear, and ASUS.

PirateFi, a Steam game, was found spreading Vidar malware, stealing user data. Steam removed it, but gamers must take urgent security steps, according to an article from TechRepublic. Earlier this month, researchers discovered that a free-to-play game called PirateFi was distributing the Vidar information-stealing malware to users on gaming platform Steam. From Feb. 6-12, as many as 1,500 users downloaded the game before Steam removed it from the platform.

Screenshot Showcase

Posted by astronaut, on February 5, 2025, running openbox.

PCLinuxOS Recipe Corner

Easy Baked Salsa Chicken and Rice

Serves: 4

INGREDIENTS:

1 tablespoon olive oil
4 chicken breasts (about 3 oz each)
1 tablespoon low sodium taco seasoning
2 bell peppers (I use red and green) chopped
1 1/4 cup long grain white rice
3 cups low sodium chicken stock
1 1/2 cups salsa
1/2 cup shredded cheddar cheese
Avocados, sour cream, chopped cilantro and sliced jalapeños for serving optional

DIRECTIONS:

Preheat your oven to 375 degrees Fahrenheit.

Heat a large oven-safe skillet over high heat and add the olive oil.

Sprinkle the 4 chicken breasts with the taco seasoning on both sides and sear the chicken in the pan on both sides. The chicken breasts will only need about 2 minutes per side over high heat - the idea is not to cook the chicken through, but just to develop some flavor on the outside of the chicken and in the pan. (Feel free to skip this step to save time - see recipe tips)

Turn off the heat under the pan. Remove the chicken breasts to a plate and add the chopped bell peppers, rice, and chicken stock to the pan, stirring everything together.

Add the chicken breasts back in, nestling them into the rice mixture.

Spoon the salsa over top of the chicken breasts and then top them with the shredded cheese.

Add the whole pan to the oven, uncovered, for about 35–45 minutes, or until the rice is cooked, and the chicken is cooked through to an internal temperature of 165 degrees Fahrenheit or 74 degrees Celsius. (Because pans and oven temperatures vary, this can affect baking time. Use an instant-read thermometer for best results).

Once the chicken and rice are cooked through, remove the pan from the oven and serve with a sprinkling of fresh cilantro, some sliced jalapeños (optional), and even a dollop of sour cream, if desired.

TIPS:

To save time, skip the step of browning the

chicken breasts in the pan. Simply add the raw chicken breasts into the rice mixture, top with salsa and cheese, and bake.

Serve with a green salad and a nice crusty bread or sweet cornbread.

If you are lucky and have leftovers, You can store them in an airtight container for up to 5 days.

This salsa chicken recipe makes a great freezer meal:

* Assemble salsa chicken according to recipe directions but don't add the cheese.
* Double wrap in plastic wrap, then double wrap in foil.
* Freeze for up to 3 months.
* When ready to bake, defrost in the refrigerator overnight, then let sit on the counter for 20 minutes before baking.
* Bake according to recipe directions, adding another 10 minutes to the cooking time.

NUTRITION:

Calories: 633 Carbs: 59g Sodium: 1146 mg
Fiber: 4g Protein: 61g

Screenshot Showcase

Posted by brisvegas, on February 1, 2025, running Mate.

The PCLinuxOS Magazine

Created with Scribus

Repo Review: A Detailed Look At Grsync

by kalwisti (David Pardue)

March 31st is World Backup Day: the day to prevent data loss! It is celebrated annually on the day before April Fool's Day, as a reminder that we will be fooled if we do not regularly back up our data. Your data is the most valuable part of your computer. A computer, its operating system and programs can be replaced, but you cannot replace lost family photos, your writing projects or financial records without a backup. Data loss can be caused by hard drive crashes, system failure or by accidents (user error) — not to mention that 21% of people have never bothered to make a backup.

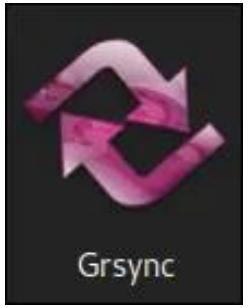
This article was inspired by a simple Grsync tutorial which was originally written by Iain Jackson for the August 2007 issue of our community magazine, and updated by Paul Arnote in November 2009. To commemorate the holiday, I decided to "refresh" these articles by covering Grsync in more detail and discussing a few aspects of the program that confused me at first.

Texstar has frequently recommended that users should follow a two-pronged backup strategy: Timeshift to take care of the operating system files (i.e., everything except for your /home directory) and another backup utility — such as Grsync, Back In Time or luckyBackup — for your personal data (i.e., documents, pictures, music, videos).

I personally use Grsync on my PCLinuxOS Xfce system and Back In Time on my LXQt machine. I have never tried the Qt-based luckyBackup, but I have read favorable comments about it. (luckyBackup's last stable release [ver. 0.5.0] dates from 2018; while development is "almost frozen", the program is still supported by its developer).

You might be wondering … "Why do I need two different backup applications? Why can't I just use Timeshift for everything?"

If you use a single solution such as Timeshift, when you need to restore your system (after a borked upgrade, for instance), Timeshift will also overwrite your documents to a **previous** / **earlier** state — something you definitely want to avoid. However, if you have separate backups for your OS and your personal files, you can just have Timeshift revert to a previous working state without affecting your current documents.



Grsync (short for "Gnome-Rsync") is a GUI for the command-line rsync utility. Although rsync is very powerful, it uses a complex set of arguments that can be overwhelming for the average user. Grsync makes use of the GTK toolkit and can run under Xfce, MATE and GNOME as well as Qt desktop environments (KDE, LXQt). Its primary developer, Piero Orsoni, believed that a graphical user interface would provide more opportunity for interaction with rsync by creating visual markers — including checkboxes, transfer processing visuals, and text entries.

Grsync is a mature, robust program. It was initially released in December 2005 and is FOSS (licensed under the GPL). We have the most recent version, 1.3.1, available in the PCLinuxOS repositories. Orsoni's work has been recognized for its quality. Linux Journal awarded Grsync the Editors' Choice Award in January 2013.

Preparation: Choose a File System for Your Destination Drive

Ext4

Before using Grsync to back up your **/home** directory, you will need to decide which file system to use on your destination/target drive. For backing up an entire directory, it is better to

format your backup medium with a native Linux file system, such as ext4. ext4 is suitable for both internal and removable drives.

This helps ensure that things such as permissions, groups, time stamps and such are preserved. The **ext4** file system also has journaling, which means that if your device is unplugged prematurely, there is more of a chance that the damaged filesystem can be recovered.

When using an ext4 file system across multiple computers, however, one issue to keep in mind is permissions. If the different computers do not have the same set of users with the same UIDs (User IDs), the ownership will be wrong. Linux does not care about your user name when deciding who owns files. Instead, it pays attention to the file's numeric User ID.

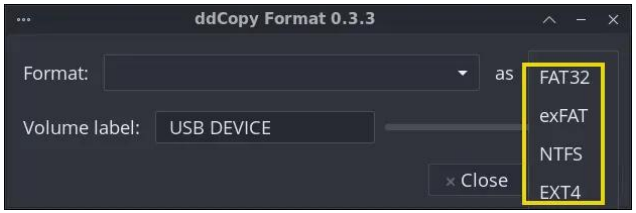
As a hypothetical example, let's say your User ID is 1000 on one computer, and 1001 on another PC. If you create files on your external drive on the first machine, those files will be owned by user 1000 — which is you. When you plug the drive into the other computer, those files are not owned by you any longer, since you are User 1001 on that second machine. Instead, the files belong to User 1000 (who is someone else).

The solution: Check your User ID and coordinate User IDs between your computers. You can easily determine your UID by typing this command in a Terminal: $ id -u *yourusername*

If you are the sole user on your PCLinuxOS computer, this command should return a value of "1000". Typically, the User ID created for users on Linux systems now starts from 1000. So, a user with UID 1000 is the first normal user (non-root user) created on the system. (I checked my Linux boxes and this was true with Mint 22.1, Debian 12 Bookworm and Slackware 15.0).

If necessary, you should be able to change User IDs using the usermod command.

If you choose ext4 as your file system, you can format your backup drive with GParted or with PCLinuxOS's own utility, ddCopy. (Look under the program's **Format USB Device** tab.)



If you wish, you can instruct GParted to set a name for the USB backup partition ("Backups" for example).

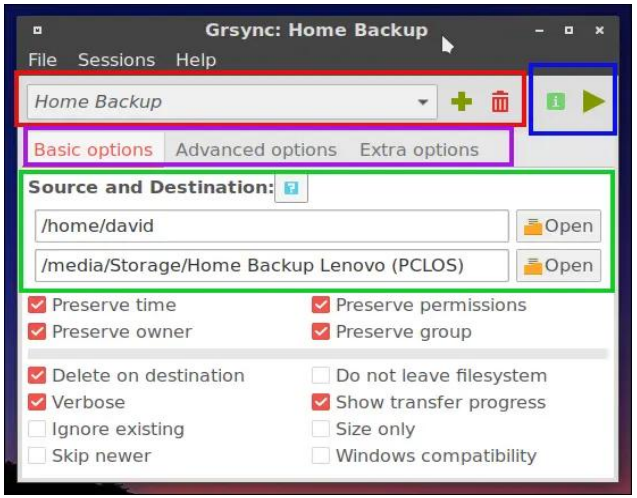
FAT32

However, if you need a backup device with broader compatibility — meaning that it can plug into any computer at any time, then FAT32 is an option. Most USB flash drives come with FAT (File Allocation Table) as the default file system. FAT32 is the "lowest common denominator" which also allows you to share files with Windows PCs or macOS. Be aware, though, that FAT32 can only store files smaller than 4 GB; it lacks journaling and does not support file attributes such as permissions.

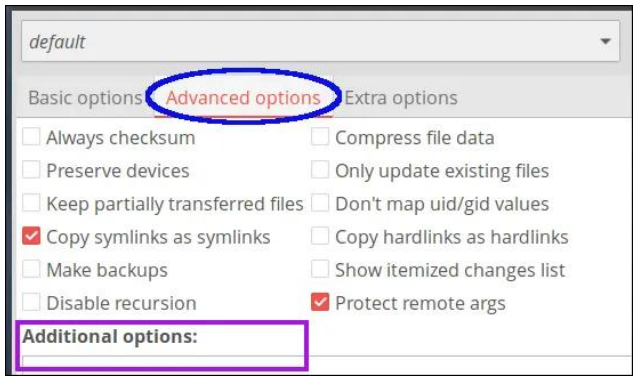
Grsync's Interface

Once you have prepared/formatted your backup drive and have installed Grsync via the Synaptic Package Manager, you are ready to begin using Grsync.

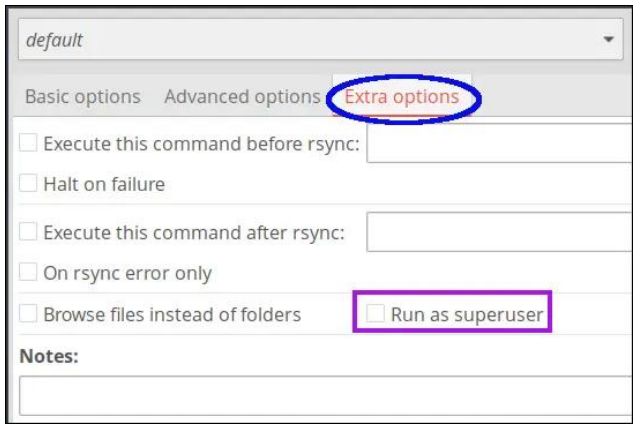
Grsync has a compact UI that displays multiple elements: a Profile bar (outlined in **red**); an "Action" area (outlined in **blue**); the Source and Destination area (outlined in **green**); and three Tabs with different options (outlined in **purple**):



The "Basic options" tab (shown above) displays when Grsync is started. Clicking on the "Advanced options" tab will bring it forward. (I will discuss the various options in more detail, as I walk through the backup process.)



Below is a screenshot of the "Extra options" tab:



Profile Bar

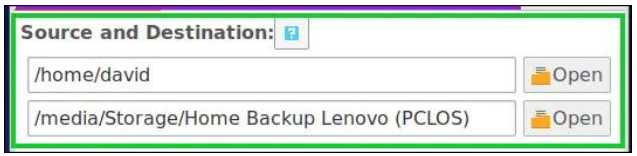
By default, the Profile Bar shows a Backup Session named "default" (since it does not know how you plan to structure your backup). Clicking on the plus sign/icon (+) will create a new backup session that you can customize to suit your needs, and save it as a Profile. (This allows you to quickly run the same backup routine in the future.)

Each Profile has its own settings, and you may create as many profiles as you wish. For example, you can create one profile to back up your entire /home directory, another profile to back up just your photographs and yet another profile for backing up your digital music.

For simplicity's sake, I will assume that you intend to back up your entire /home directory. Click on the plus sign (+) to add a new session and type in a session name like "Home Backup".

Source and Destination Directories

Next, you must add your **Source and Destination** directories. There are two boxes in the middle of the Grsync UI. The top box is the Source — this is where your files currently are. The bottom box is the Destination — where you want your files backed up to.

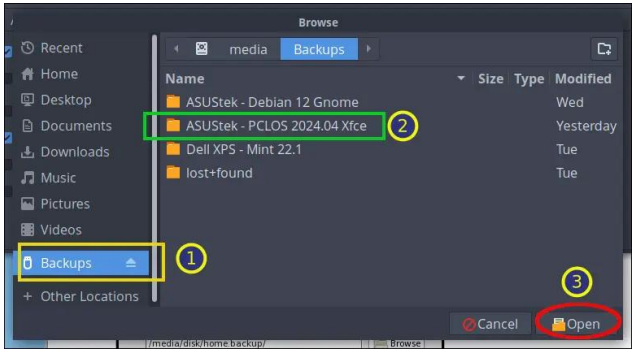


If you wish to back up to a removable medium such as a USB flash drive or external USB drive, insert it now. Wait a moment until PCLinuxOS detects the drive and mounts it.

It is a good idea to create a new directory on your removable disk to store the backup files. You may name it whatever you like. I use the directory name "PCLOS 2024.04 Xfce" (since I use this same flash drive to back up the /home files from my Debian Bookworm system and my Mint 22.1 system).

Click on the **Open** button beside the **Source** box. This should take you straight to your /home directory. Just click on **Open** to select it.

Click on the **Open** button next to the **Destination** box. Your removable drive should appear as an entry in the left-hand margin of the file manager dialog, for easy access. Click on the removable drive entry to select it, then click on your desired backup folder before choosing the **Open** button.



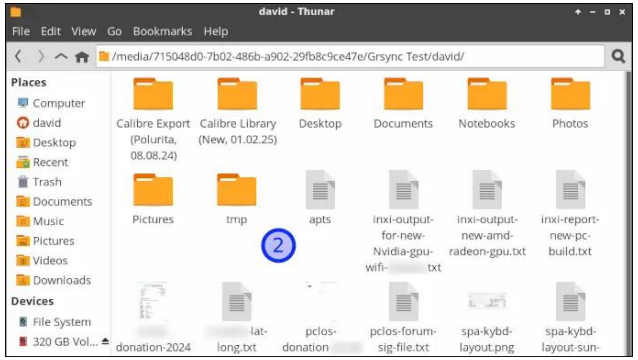
The Perplexing "Trailing Slash"

I must digress for a moment to discuss a confusing aspect of Grsync: the presence — or absence — of a trailing slash on the Source directory. I struggled to understand this correctly (and it still trips me up on occasion). The reason that Grysnc cares about this is because rsync is running under the hood, and rsync is persnickety about the trailing slash in the Source (directory) argument.

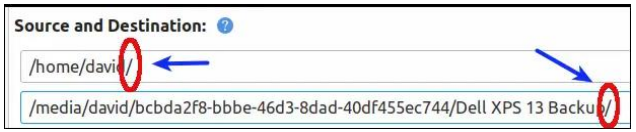
Two concrete examples will hopefully demonstrate the use of the trailing slash when copying your /home directory.

In the scenario below, the trailing slash is **omitted** from the Source directory (/home/david) which will be copied:

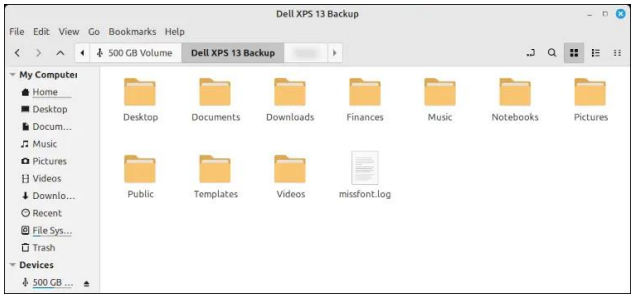
The result of this setting will be that Grsync copies the Source directory (/david) to the Destination. Another way of phrasing this, is that Grsync will copy the Source directory itself [*Screenshot 1*] and all its contents (subdirectories) [*Screenshot 2*]:



In our second scenario below, the trailing slash is **added** to the Source directory (/home/david) which will be copied:



The presence of the trailing slash instructs rsync to avoid creating an additional directory level at the Destination drive. The result is that (G)rsync will **not** add "david" as a parent directory, but it will copy all of david's subdirectories with their contents:



My takeaway is:

1. Add a trailing slash in the Source box if you are backing up all the personal files in your / home directory (including personal folders such as Documents, Photos, Music, etc.)

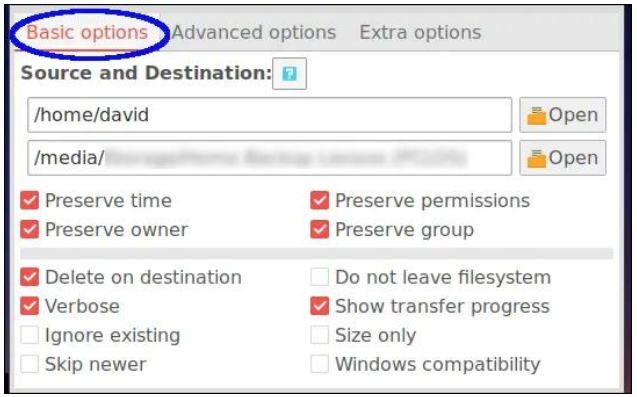
2. Omit a trailing slash from the Source box — and select "Run as superuser" [under the **Extra options** tab] — if you are backing up multiple user accounts' files (such as your account, your spouse's account and/or your children)

3. If you are just backing up the contents of a **sub**directory within your /home directory (e.g., Documents) and wish to retain the parent Documents directory as a "container" for those files, then omit a trailing slash from the Source box.

The trailing slash's behavior is not a life-or-death situation. Grsync will back up your files regardless of how you handle the trailing slash. However, you can better achieve your intended backup result if you understand how the trailing slash functions. I recommend that you make some practice backups, using different options, to gain confidence using Grsync.

Basic Options Tab

Now it's time to examine some of Grsync's **Basic options** — and change them, if you wish.



Preserve owner/permissions/group: This is optional if you are just backing up your /home directory (or a specific folder with some of your data files). Selecting just the "Preserve time"

option is sufficient. However, it will not be harmful to select these options during a backup, so I check/tick them.

If you are backing up multiple user accounts' files, it is important to select these options — since the other users have different permissions than you.

Delete on destination (*Optional*): Selecting this option ensures that you will not end up with any old files in your backup that do not exist in your /home directory. If you delete a file from your /home folder and then perform a backup, Grsync will also delete that file on the Destination.

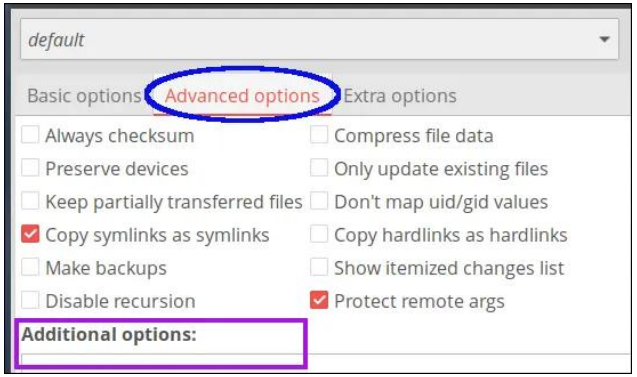
Verbose: This is selected by default. It instructs Grsync to show more information when you perform a dry-run prior to your actual backup.

Show transfer progress: This is selected by default. It tells Grsync to display a progress bar during the transfer/backup process.

Skip newer (*Optional*): If you have newer files in the Destination compared to the Source, those files will not be updated.

Windows compatibility (*Optional*): If selected, this provides a workaround for a Windows FAT file system limitation. The copy will be made such that Linux files will be compatible with the NTFS file system.

Advanced Options Tab



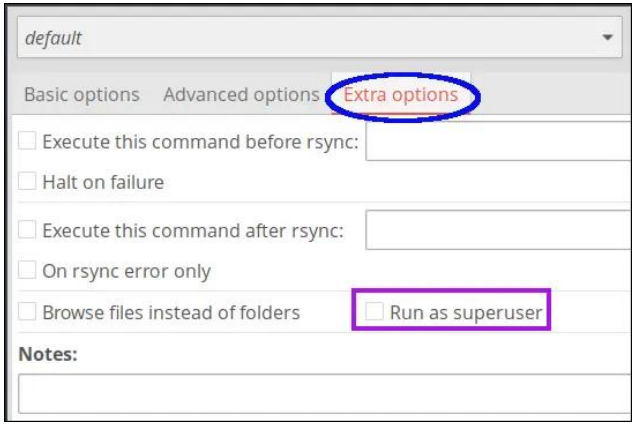
Although there are numerous options listed, I believe that you will likely deal with just three of them in ordinary use.

Copy symlinks as symlinks: This means that if there are any links to files, only the link, rather than the file itself, is copied over. I recommend that you select this option.

Protect remote args: This is selected by default, so I leave it as is. If you hover your mouse cursor over the option, a tooltip with a geeky explanation (which is beyond my understanding) will display.

Additional options: In this box, you may type additional commands to pass to rsync. This is useful if you wish to exclude specific folders from your backup. I will provide examples of the "--exclude" command shortly.

Extra Options Tab



Run as superuser (*Optional*): You do **not** need to select this option if you are only backing up your personal files/folders. However, if you are backing up multiple user accounts' files, you should check/tick it.

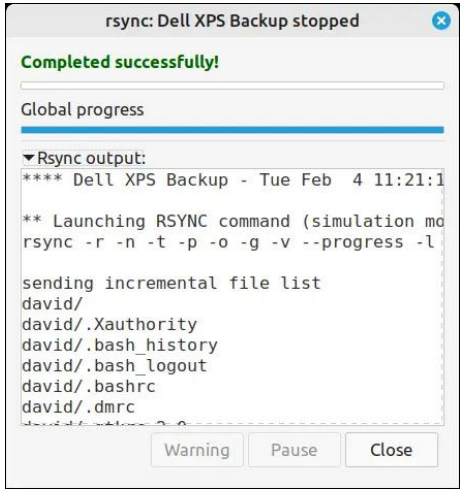
If you select this option, Grsync will prompt you to authenticate with root credentials before you can create the backup.

Simulation/Dry Run

After creating a Backup Session, specifying your Source and Destination, and choosing your desired options, it is finally time to perform the backup. One of Grsync's most useful features is its Simulation mode (also known as a "dry run" mode).

The dry run is a safety feature that shows what will be copied over to your Destination — without actually doing it. This is a great way to

test your session and tweak the backup parameters without the risk of destroying your data. The Simulation icon is located in the "Action" area of the toolbar (upper-right corner):



When you are satisfied that all the correct files are being either deleted or copied, click on the **Make a Full Run/Go** icon in the toolbar:

The first time you run the sync it may take a while, as it has to transfer all your data. The exact time will depend upon the amount of data you are copying and the speed of your computer. It might take 5–10 minutes to transfer your / home the first time out — longer if you have many large files such as music or video files. Subsequent syncs will be much quicker (perhaps 30 seconds) as Grsync only sends new or updated files for backup.

Grsync's incremental backup process gives it a significant advantage over a manual backup. There is no substitute for seeing this feature in action, to fully appreciate it. The Linux for Seniors video tutorial on Grsync demonstrates incremental backup from minute 11:57 until 13:45 and from minute 14:01 until 17:58.

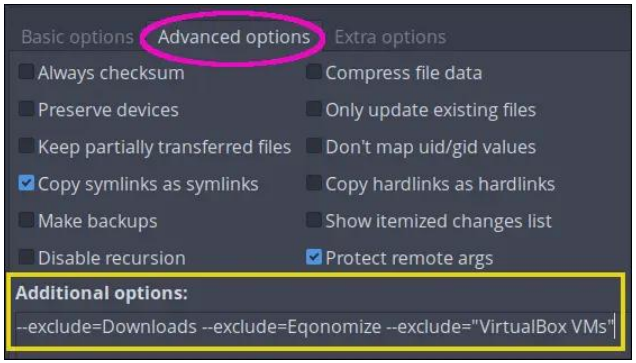
Grsync offers yet another advantage: it makes an exact copy of your Source files in your selected Destination. Your files are directly accessible. There is no need to access them via Grsync itself. In other words, you can open/copy/move your files without having to use Grsync.

If you need to restore from a backup created with Grsync, you can either use its Restore function (under the **File** menu > choose **Switch source with destination**), or you can open the storage device with your DE's file manager, and manually copy the files that you want.

Excluding Folders from Your Backup

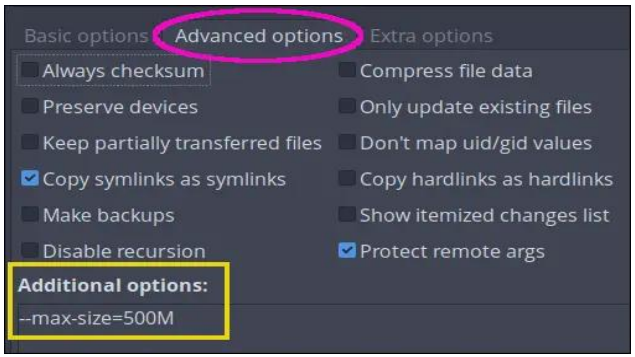
You may exclude directories/folders from your backup, if you wish. Under the **Advanced options** tab, there is a box labeled "**Additional options.**" It is a free-text field that allows you to specify extra options not listed in Grsync's GUI.

The "--exclude" option of rsync will exclude directories that you decide to omit from your backup, such as the Downloads folder (where I often store bulky Linux ISO files which can be re-downloaded if necessary), the Eqonomize folder (an AppImage) and the large virtual machines directory:



If your directory name has spaces, remember to enclose it within quotation marks. (Single quotation marks [' '] also work fine, based on my testing.)

Another handy option is the ability to specify a maximum file size that Grsync will copy, such as the example below, which limits the file size to 500 MB. In other words, anything larger than 500 MB will not be backed up:



Additional Resources

Average Linux User [Vladimir Mikulić]. "Linux Backup with Graphical Programs." YouTube, 4 Oct. 2017. A clear and concise tutorial. He covers Grsync from minute 1:33 until 12:14.

EzeeLinux [Joe Collins]. "Linux Tip: Making Backups with Grsync." YouTube, 18 Apr. 2015. (16 min., 1 sec.)

Linux for Seniors [Thor Hartmannsson]. "Kubuntu — KDE Plasma: Tips Using Grsync for Backups." YouTube, 2 May 2023. (18 min., 22 sec.) Helpful for its real-time demonstration of incremental backup, from minute 11:57 until 13:45 and 14:01 until 17:58.

Conclusion

Grsync is a wonderful tool for helping you establish a backup routine. According to World Backup Day's website and other online sources, losing your files is a common occurrence. Considering that millions of computers will fail this year or be infected with malware, and that some people have never made an effort to back up, it's not a question of "if" you're going to lose your data, but "when." Give yourself some peace of mind by creating a backup with Grsync on March 31st and making a resolution to back up regularly. Ideally, you should follow the "3-2-1" Backup Rule to ensure that your data is protected.

Screenshot Showcase

Posted by francesco_bat, on February 5, 2025, running icewm.

On The Precipice: The Battle Between AI & Copyright

by Tori Noble
Electronic Frontier Foundation

Part One: Copyright and AI: the Cases and the Consequences

The launch of ChatGPT and other deep learning quickly led to a flurry of lawsuits against model developers. Legal theories vary, but most are rooted in copyright: plaintiffs argue that use of their works to train the models was infringement; developers counter that their training is fair use. Meanwhile, developers are making as many licensing deals as possible to stave off future litigation, and it's a sound bet that the existing litigation is an elaborate scramble for leverage in settlement negotiations.

These cases can end one of three ways: rightsholders win, everybody settles, or developers win. As we've noted before, we think the developers have the better argument. But that's not the only reason they should win these cases: while creators have a legitimate gripe, expanding copyright won't protect jobs from automation. A win for rightsholders or even a settlement could also lead to significant harm, especially if it undermines fair use protections for research uses or artistic protections for creators. In this article and a follow-up, we'll explain why.

State of Play

First, we need some context, so here's the state of play:

DMCA Claims

Multiple courts have dismissed claims under Section 1202(b) of the Digital Millennium Copyright Act, stemming from allegations that developers removed or altered attribution information during the training process. In *Raw Story Media v. OpenAI, Inc.*, the Southern District of New York dismissed these claims because the plaintiff had not "plausibly alleged" that training ChatGPT on their works had actually harmed them, and there was no "substantial risk" that ChatGPT would output their news articles. Because ChatGPT was trained on "massive amounts of information from innumerable sources on almost any given subject…the likelihood that ChatGPT would output plagiarized content from one of Plaintiffs' articles seems remote." Courts granted motions to dismiss similar DMCA claims in *Andersen v. Stability AI, Ltd.*, *The Intercept Media, Inc. v. OpenAI, Inc.*, *Kadrey v. Meta Platforms, Inc.*, and *Tremblay v. OpenAI*.

Another such case, *Doe v. GitHub, Inc.* will soon be argued in the Ninth Circuit.

Copyright Infringement Claims

Rightsholders also assert ordinary copyright infringement, and the initial holdings are a mixed bag. In *Kadrey v. Meta Platforms, Inc.*, for example, the court dismissed "nonsensical" claims that Meta's LLaMA models are themselves infringing derivative works. In *Andersen v. Stability AI Ltd.*, however, the court held that copyright claims based on the assumption that the plaintiff's works were included in a training data set could go forward, where the use of plaintiffs' names as prompts generated outputted images that were "similar to plaintiffs' artistic works." The court also held that the plaintiffs plausibly alleged that the model was designed to "promote infringement" for similar reasons.

It's early in the case — the court was merely deciding if the plaintiffs had alleged enough to justify further proceedings — but it's a dangerous precedent. Crucially, copyright protection extends only to the actual expression of the author — the underlying facts and ideas in a creative work are not themselves protected. That means that, while a model cannot output an identical or near-identical copy of a training image without running afoul of copyright, it is free to generate stylistically "similar" images. Training alone is insufficient to give rise to a claim of infringement, and the court impermissibly conflated permissible "similar" outputs with the copying of protectable expression.

Fair Use

In most of the AI cases, courts have yet to consider — let alone decide — whether fair use applies. In one unusual case, however, the judge has flip-flopped, previously finding that the defendant's use was fair and changing his mind. This case, *Thomson Reuters Enterprise Centre GMBH v. Ross Intelligence, Inc.*, concerns legal research technology. Thomson Reuters provides search tools to locate relevant legal opinions and prepares annotations describing the opinions' holdings. Ross Intelligence hired lawyers to look at those annotations and rewrite them in their own words. Their output was used to train Ross's search tool, ultimately providing users with relevant legal opinions based on their queries. Originally, the court got it right, holding that if the AI developer used copyrighted works only "as a step in the process of trying to develop a 'wholly new,' albeit competing, product," that's "transformative intermediate copying," *i.e.* fair use.

After reconsidering, however, the judge changed his mind in several respects, essentially disagreeing with prior case law regarding search engines. We think it's unlikely that an appeals court would uphold this divergence from precedent. But if it did, it would present legal problems for AI developers — and anyone creating search tools.

Copyright law favors the creation of new technology to learn and locate information, even when developing the tool required copying books and web pages in order to index them. Here, the search tool is providing links to legal opinions, not presenting users with any Thomson Reuters original material. The tool is concerned with non-copyrightable legal holdings and principles, not with supplanting any creative expression embodied in the annotations prepared by Thomson Reuters.

Thomson Reuters has often pushed the limits of copyright in an attempt to profit off of the public's need to access and refer to the law, for instance by claiming a proprietary interest in its page numbering of legal opinions. Unfortunately, the judge in this case enabled them to do so in a new way. We hope the appeals court reverses the decision.

The Side Deals

While all of this is going on, developers that can afford it — OpenAI, Google, and other tech behemoths — have inked multimillion-dollar licensing deals with Reddit, the Wall Street Journal, and myriad other corporate copyright owners. There's suddenly a $2.5 billion licensing market for training data — even though the use of that data is almost certainly fair use.

What's Missing

This litigation is getting plenty of attention. And it should because the stakes are high. Unfortunately, the real stakes are getting lost. These cases are not just about who will get the most financial benefits from generative AI. The outcomes will decide whether a small group of

corporations that can afford big licensing fees will determine the future of AI for all of us.

Part Two: AI and Copyright: Expanding Copyright Hurts Everyone — Here's What to Do Instead

You shouldn't need a permission slip to read a webpage – whether you do it with your own eyes, or use software to help. AI is a category of general-purpose tools with myriad beneficial uses. Requiring developers to license the materials needed to create this technology threatens the development of more innovative and inclusive AI models, as well as important uses of AI as a tool for expression and scientific research.

Threats to Socially Valuable Research and Innovation

Requiring researchers to license fair uses of AI training data could make socially valuable research based on machine learning (ML) and even text and data mining (TDM) prohibitively complicated and expensive, if not impossible. Researchers have relied on fair use to conduct TDM research for a decade, leading to important advancements in myriad fields. However, licensing the vast quantity of works that high-quality TDM research requires is frequently cost-prohibitive and practically infeasible.

Image by Mohamed Hassan from Pixabay

Fair use protects ML and TDM research for good reason. Without fair use, copyright would hinder important scientific advancements that benefit all of us. Empirical studies back this up: research using TDM methodologies are more common in countries that protect TDM research from copyright control; in countries that don't, copyright restrictions stymie beneficial research. It's easy to see why: it would be impossible to identify and negotiate with millions of different copyright owners to analyze, say, text from the internet.

The stakes are high, because ML is critical to helping us interpret the world around us. It's being used by researchers to understand everything from space nebulae to the proteins in our bodies. When the task requires crunching a huge amount of data, such as the data generated by the world's telescopes, ML helps rapidly sift through the information to identify features of potential interest to

researchers. For example, scientists are using AlphaFold, a deep learning tool, to understand biological processes and develop drugs that target disease-causing malfunctions in those processes. The developers released an open-source version of AlphaFold, making it available to researchers around the world. Other developers have already iterated upon AlphaFold to build transformative new tools.

Threats to Competition

Requiring AI developers to get authorization from rightsholders before training models on copyrighted works would limit competition to companies that have their own trove of training data, or the means to strike a deal with such a company. This would result in all the usual harms of limited competition — higher costs, worse service, and heightened security risks — as well as reducing the variety of expression used to train such tools and the expression allowed to users seeking to express themselves with the aid of AI. As the Federal Trade Commission recently explained, if a handful of companies control AI training data, "they may be able to leverage their control to dampen or distort competition in generative AI markets" and "wield outsized influence over a significant swath of economic activity."

Legacy gatekeepers have already used copyright to stifle access to information and the creation of new tools for understanding it. Consider, for example, *Thomson Reuters v. Ross Intelligence*, widely considered to be the first lawsuit over AI training rights ever filed. Ross Intelligence sought to disrupt the legal research duopoly of Westlaw and LexisNexis by offering a new AI-based system. The startup attempted to license the right to train its model on Westlaw's summaries of public domain judicial opinions and its method for organizing cases. Westlaw refused to grant the license and sued its tiny rival for copyright infringement. Ultimately, the lawsuit forced the startup out of business, eliminating a would-be competitor that might have helped increase access to the law.

Similarly, shortly after Getty Images — a billion-dollar stock images company that owns hundreds of millions of images — filed a copyright lawsuit asking the court to order the "destruction" of Stable Diffusion over purported copyright violations in the training process, Getty introduced its own AI image generator trained on its own library of images.

Requiring developers to license AI training materials benefits tech monopolists as well. For giant tech companies that can afford to pay, pricey licensing deals offer a way to lock in their dominant positions in the generative AI market by creating prohibitive barriers to entry. To develop a "foundation model" that can be used to build generative AI systems like ChatGPT and Stable Diffusion, developers need to "train" the model on billions or even trillions of works, often copied from the open internet without permission from copyright holders. There's no feasible way to identify all of those rightsholders — let alone execute deals with each of them. Even if these deals were possible, licensing that much content at the prices developers are currently paying would be prohibitively expensive for most would-be competitors.

We should not assume that the same companies who built this world can fix the problems they helped create; if we want AI models that don't replicate existing social and political biases, we need to make it possible for new players to build them.

Nor is pro-monopoly regulation through copyright likely to provide any meaningful economic support for vulnerable artists and creators. Notwithstanding the highly publicized demands of musicians, authors, actors, and other creative professionals, imposing a licensing requirement is unlikely to protect the jobs or incomes of the underpaid working artists that media and entertainment behemoths have exploited for decades. Because of the imbalance in bargaining power between creators and publishing gatekeepers, trying to help creators by giving them new rights under copyright law is, as EFF Special Advisor Cory Doctorow has written, like trying to help a bullied kid by giving them more lunch money for the bully to take.

Entertainment companies' historical practices bear out this concern. For example, in the late-2000's to mid-2010's, music publishers and recording companies struck multimillion-dollar direct licensing deals with music streaming companies and video sharing platforms. Google reportedly paid more than $400 million to a single music label, and Spotify gave the major record labels a combined 18 percent ownership interest in its now-$100 billion company. Yet

music labels and publishers frequently fail to share these payments with artists, and artists rarely benefit from these equity arrangements. There is no reason to believe that the same companies will treat their artists more fairly once they control AI.

Threats to Free Expression

Generative AI tools like text and image generators are powerful engines of expression. Creating content—particularly images and videos—is time intensive. It frequently requires tools and skills that many internet users lack. Generative AI significantly expedites content creation and reduces the need for artistic ability and expensive photographic or video technology. This facilitates the creation of art that simply would not have existed and allows people to express themselves in ways they couldn't without AI.

Some art forms historically practiced within the African American community — such as hip hop and collage — have a rich tradition of remixing to create new artworks that can be more than the sum of their parts. As professor and digital artist Nettrice Gaskins has explained, generative AI is a valuable tool for creating these kinds of art. Limiting the works that may be used to train AI would limit its utility as an artistic tool, and compound the harm that copyright law has already inflicted on historically Black art forms.

Generative AI has the power to democratize speech and content creation, much like the internet has. Before the internet, a small number of large publishers controlled the channels of speech distribution, controlling which material reached audiences' ears. The internet changed that by allowing anyone with a laptop and Wi-Fi connection to reach billions of people around the world. Generative AI magnifies those benefits by enabling ordinary internet users to tell stories and express opinions by allowing them to generate text in a matter of seconds and easily create graphics, images, animation, and videos that, just a few years ago, only the most sophisticated studios had the capability to produce. Legacy gatekeepers want to expand copyright so they can reverse this progress. Don't let them: everyone deserves the right to use technology to express themselves, and AI is no exception.

Threats to Fair Use

In all of these situations, fair use — the ability to use copyrighted material without permission or payment in certain circumstances — often provides the best counter to restrictions imposed by rightsholders. But, as we explained in the first post in this series, fair use is under attack by the copyright creep. Publishers' recent attempts to impose a new licensing regime for AI training rights—despite lacking any recognized legal right to control AI training—threatens to undermine the public's fair use rights.

By undermining fair use, the AI copyright creep makes all these other dangers more acute. Fair use is often what researchers and educators rely on to make their academic assessments and to gather data. Fair use allows competitors to build on existing work to offer better alternatives. And fair use lets anyone comment on, or criticize, copyrighted material.

When gatekeepers make the argument against fair use and in favor of expansive copyright—in court, to lawmakers, and to the public—they are looking to cement their own power, and undermine ours.

A Better Way Forward

AI also threatens real harms that demand real solutions.

Many creators and white-collar professionals increasingly believe that generative AI threatens their jobs. Many people also worry that it enables serious forms of abuse, such as AI-generated non-consensual intimate imagery, including of children. Privacy concerns abound, as does consternation over misinformation and disinformation. And it's already harming the environment.

Expanding copyright will not mitigate these harms, and we shouldn't forfeit free speech and innovation to chase snake oil "solutions" that won't work.

We need solutions that address the roots of these problems, like inadequate protections for labor rights and personal privacy. Targeted, issue-specific policies are far more likely to succeed in resolving the problems society faces. Take competition, for example. Proponents of

copyright expansion argue that treating AI development like the fair use that it is would only enrich a handful of tech behemoths. But imposing onerous new copyright licensing requirements to train models would lock in the market advantages enjoyed by Big Tech and Big Media — the only companies that own large content libraries or can afford to license enough material to build a deep learning model — profiting entrenched incumbents at the public's expense. What neither Big Tech nor Big Media will say is that stronger antitrust rules and enforcement would be a much better solution.

What's more, looking beyond copyright future-proofs the protections. Stronger environmental protections, comprehensive privacy laws, worker protections, and media literacy will create an ecosystem where we will have defenses against any new technology that might cause harm in those areas, not just generative AI.

Expanding copyright, on the other hand, threatens socially beneficial uses of AI — for example, to conduct scientific research and generate new creative expression — without meaningfully addressing the harms.

A Bash Script Program Launcher For The Notification Area Of Your Panel

by Paul Arnote (parnote)

I have to be completely honest about something. I ***love*** messing around with bash scripts. They play right into my quest to solve problems and save time. It also harkens back to my days when I was a burgeoning shareware programmer that started way back when I was using Windows 3.1. Trust me … I didn't get rich off of the shareware I wrote (not even close).

With my bash scripts, I'm able to accomplish repetitive tasks with a minimum of effort. One example is the bash script that I wrote (and use monthly) to create the various sized images used for the magazine's HTML layout. And I have not one, but two versions of that script. One creates the various sized JPG files from the PNG file produced by Scribus. The other creates a PNG file from the actual PDF, and then I run the other script on that PNG file to create the various sized JPG files.

I have well over a dozen bash scripts that I use as the "motor" for quite a few Thunar Custom Actions. I've featured most of them here in the pages of this magazine, in fact. Many of my bash scripts have GUI elements to prompt for input, or to display the progress of the task being handled. And, to be quite frank about it, I tend to use Zenity over yad a LOT more often to handle/display those GUI elements, probably mostly out of my increased familiarity with Zenity. I should probably try to use yad more, because it has a LOT more options and capabilities than Zenity. Kdialog (the third set of GUI elements available in the PCLinuxOS repository for use from a bash script, from the KDE developers) has a set of instructions/commands that's even more sparse than Zenity, and a whole different usage format, as well.

I'm definitely not a command line commando, nor am I a bash warrior. But there is a great sense of accomplishment to streamline several tedious and mundane tasks into one bash script. I definitely have a LOT more to learn when it comes to both (the command line and bash scripting). I just look at it as a work-in-progress. For example, I'm super weak in my understanding of how to properly use sed or awk. Eventually, I'll get it.

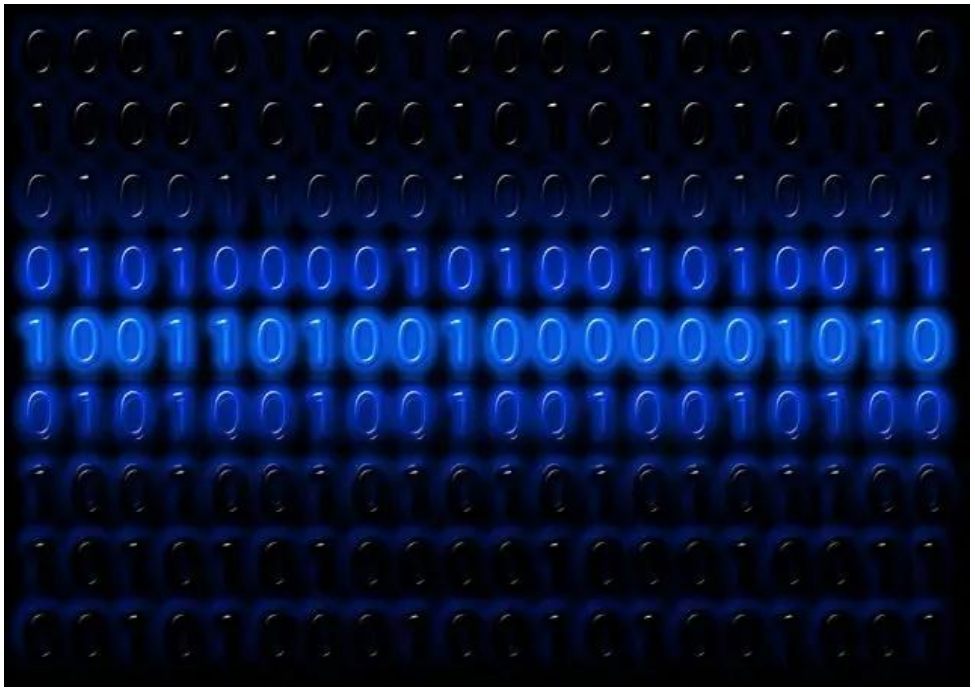


Image by Gerd Altmann from Pixabay

One of the things I've been pursuing with my bash scripting is how to create an interactive script that runs in the notification tray of my Xfce panel. I'm not just talking about displaying text in a notification popup. Any eight-year-old can do that with one simple command. I mean something you can **truly** interact with. Up to this point, it has become my bash scripting "holy grail."

For the longest time, I thought that was virtually impossible, without having to write a full program in C, and all of the things that go along with that whole process. I felt like there certainly had to be a way to do so from a bash script.

I searched for YEARS to figure out how to do this. And, I was blown away by how simple it actually is. You won't believe this, but it's literally a one-liner bash script. I found it hard to believe, too.

This script places a launcher in the notification tray of your panel. Sure, I could have just created another launcher for this on my panel, but what's the fun of that? Anyone can do that. This is a "proof of concept" thing for me.

While I'm not a "gamer," I do like to play a few games. Not only does it help keep my mind active in retirement, but it also provides a nice diversion from magazine duties. Playing the games also helps me overcome writer's block, a visitor who visits way too often.

So, my launcher contains five games that I like to play to pass time. You could, however, have whatever programs you want in this launcher. If there are programs you routinely use and that you want frequent or easy access to, those are definitely candidates for inclusion in your notification area launcher.

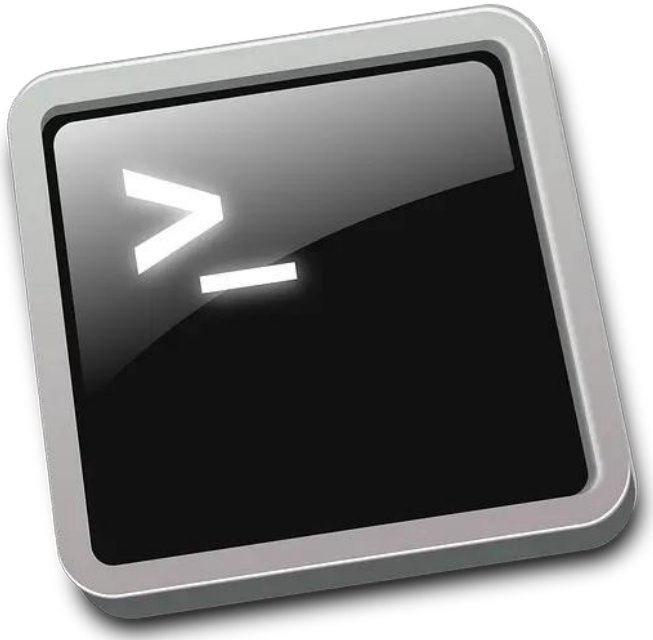


Image by OpenClipart-Vectors from Pixabay

So, here's my bash script, which I call "game-launcher.sh." The entire script is only 333 bytes long. It's short enough that I'm NOT providing a download for it. Typing it in should take you all of five minutes or less in a plain text editor. (That means NOT LO-Writer, or any other word processing program). Personally, I like/prefer Geany (it's in the PCLinuxOS repository), since it does a GREAT job of helping you avoid typing errors when writing/entering bash scripts with its colored text highlighting.

```
#!/bin/bash

yad --notification \
  --image="applications-games" \
  --text="My Fav Games" \
  --menu="PySol!pysol!pysol
  |GMahjongg!gnome-mahjongg!gnome-mahjongg
  |Gweled!gweled!gweled
  |Peg-E!peg-e!peg-e
  |Space Cadet Pinball!flatpak run com.github.k4zmu2a.
spacecadetpinball!pinball
  |Quit!quit!gtk-quit" \
  --command="menu"
```

The "space" and "backslash" at the end of the command parameters makes it easier to read (and edit). If you want to list it all out on one line, it would look something like this:

```
#!/bin/bash

yad --notification --image="applications-games" --text="My Fav
Games" --menu="PySol!pysol!pysol|GMahjongg!gnome-mahjongg!gnome-
mahjongg|Gweled!gweled!gweled|Peg-E!peg-e!peg-e|Space Cadet
Pinball!flatpak run com.github.k4zmu2a.spacecadetpinball!pinball|
Quit!quit!gtk-quit" --command="menu"
```

As you can see from reading the bash code, my launcher lists PySol, GMahjongg, Gweled, Peg-E, and a flatpak of Space Cadet Pinball.

So, let's walk through the code, step-by-step. Of course, it starts off with the typical bash shebang (#!/bin/bash). Next, we call on "yad." Yad (which stands for Yet Another Dialog) is responsible for allowing us to have an interactive presence in the notification area with a bash script.

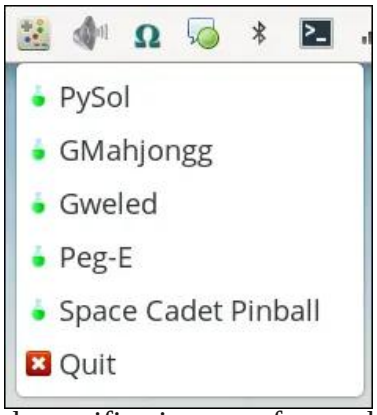
The first parameter is "--notification." This allows us to place what follows in the notification area. The second parameter, "--image," tells yad what icon to use as the icon in the notification area. The third parameter, "--text," defines the text that will appear in the popup that is displayed when we hover the mouse cursor over the icon.

The fourth parameter is where all the "magic" occurs. The "--menu" parameter defines the menu that appears when we right-click on the icon in the notification area. Each menu item is split up into three parts. For the first one, PySol, the first part is the name that appears in the menu. The second part is the name of the executable to launch. The third part is the icon to use to represent your menu item in the menu. Each part is separated by an exclamation mark.

A "pipe" character ("|") separates each entry in the menu. So, you can put as few or as many items into the menu as you like. The last entry in the menu is "Quit," which allows you to exit the launcher.

Thus, each menu entry should follow this format: **[MenuText]![ExecutableName]![IconToUse]**. That's for the first menu item. Each subsequent menu item will start with the "pipe" character, "|", followed by the format specified for the first menu item.

The final part of the yad command is "--command="menu."" This allows you to choose and launch the item you select. Below (top of next column) is an image of what it looks like on my computer.



You will notice that each icon in the menu is a green raindrop, with the exception of the last item, "Quit." No matter what icon I specify, I still only get the green raindrop as the icon for each entry in the menu. Still, we specify it, because yad is expecting to find all three parts to the menu entry … the text to display in the menu, the executable name, and the icon to use. For me, this is a minor annoyance, but one I can live with. After all, my goal was to make an interactive item in the notification area from a bash script. Even with that small niggle, I feel like it's a success.

I have my script set up to launch automatically every time I log into Xfce. While I haven't tested it on any other desktop, there's no reason this script *won't* work on other desktop environments.

Summary

So, now that I've tackled my "holy grail" of bash scripting, I'm left wondering if this information can be leveraged to do more. THAT is now my new quest. I'd LOVE to be able to create something akin to Xfce's KbLEDPlugin that will tell me when one of the "lock" keys (CapsLock, NumLock, ScrollLock) is activated, from something as lightweight and easy as a bash script. We'll see, but I'm not holding my breath. But who knows what may happen, or where/when the next element of inspiration might drop into my lap.

Using this script saves me from digging through my PCLinuxOS menu to launch the games I want to play, when I want to play them. It's just a simple right click on the icon in my notification tray, and then select the program I want to run with a left click of my mouse. Like I mentioned earlier, you can put any programs you want quick access to in your menu. It doesn't have to be games. I just chose my favorite games to be in my menu selections.

Google Is On The Wrong Side Of History

by Matthew Guariglia
Electronic Frontier Foundation
Reprinted under Creative Commons license

Google continues to show us why it chose to abandon its old motto of "Don't Be Evil," as it becomes more and more enmeshed with the military-industrial complex. Most recently, Google has removed four key points from its AI principles. Specifically, it previously read that the company would not pursue AI applications involving (1) weapons, (2) surveillance, (3) technologies that "cause or are likely to cause overall harm," and (4) technologies whose purpose contravenes widely accepted principles of international law and human rights.

Those principles are gone now.

In its place, the company has written that "democracies" should lead in AI development and companies should work together with governments "to create AI that protects people, promotes global growth, and supports national security." This could mean that the provider of the world's largest search engine–the tool most people used to uncover the best apple pie recipes and to find out what time their favorite coffee shop closes–could be in the business of creating AI-based weapons systems and leveraging its considerable computing power for surveillance.

This troubling decision to potentially profit from high-tech warfare, which could have serious consequences for real lives and real people, comes after criticism from EFF, human rights activists, and other international groups. Despite its pledges and vocal commitment to human rights, Google has faced criticism for its involvement in Project Nimbus, which provides advanced cloud and AI capabilities to the Israeli government, tools that an increasing number of credible reports suggest are being used to target civilians under pervasive surveillance in the Occupied Palestinian Territories. EFF said in 2024, "When a company makes a promise, the public should be able to rely on it." Rather than fully living up to its previous human rights commitments, it seems Google has shifted its priorities.

Google is a company valued at $2.343 trillion that has global infrastructure and a massive legal department, and appears to be leaning into the current anti-humanitarian moment. The fifth-largest company in the world seems to have chosen to make the few extra bucks (relative to the company's earnings and net worth) that will come from mass surveillance tools and AI-enhanced weapons systems.

And of course we can tell why. With government money flying out the door toward

defense contractors, surveillance technology companies, and other national security and policing related vendors, the legacy companies who swallow up all of that data don't want to miss out on the feeding frenzy. With $1 billion contracts on the table even for smaller companies promising AI-enhanced tech, it looks like Google is willing to throw its lot in with the herd.

In addition to Google and Amazon's involvement with Project Nimbus, which involved both cloud storage for the large amounts of data collected from mass surveillance and analysis of that data, there are many other scenarios and products on the market that could raise concerns. AI could be used to power autonomous weapons systems, which decide when and if to pull the trigger or drop a bomb. Targeting software can mean physically aiming weapons at people identified by geolocation or by other types of machine learning like face recognition or other biometric technology. AI could also be used to sift through massive amounts of intelligence, including intercepted communications or publicly available information from social media and the internet, in order to assemble lists of people to be targeted by militaries.

Whether autonomous AI-based weapons systems and surveillance are controlled by totalitarian states or states that meet Google's definition of "democracy", is of little comfort to the people who could be targeted, spied on, or killed in error by AI technology which is prone to mistakes. AI cannot be accountable for its actions. If we, the public, are able to navigate the corporate, government, and national security secrecy to learn of these flaws, companies will fall on a playbook we've seen before: tinkering with the algorithms and declaring the problem solved.

We urge Google, and all of the companies that will follow in its wake, to reverse course. In the meantime, users will have to decide who deserves their business. As the company's most successful product, its search engine, is faltering, that decision gets easier and easier.

Screenshot Showcase

Posted by luikki, on February 4, 2025, running KDE.

Wiki Pick: Changing GRUB Boot Menu Font Size

by Dave Marshall (CoreLite)

Editor's Note: *Wiki Pick is a new monthly column highlighting one article from the PCLinuxOS Knowledge Base Wiki every month. Whenever possible (and when known), we'll attribute the Wiki Pick article to the PCLinuxOS user who made the Wiki post. The Wiki cannot survive and thrive without the efforts of PCLinuxOS members contributing and keeping it updated. So, visit and contribute to YOUR PCLinuxOS Knowledge Base Wiki!*

While this article is relevant to PCLinuxOS Debian Edition with KDE, it should also work with the Classic RPM edition with KDE, as well as many other desktop environments.

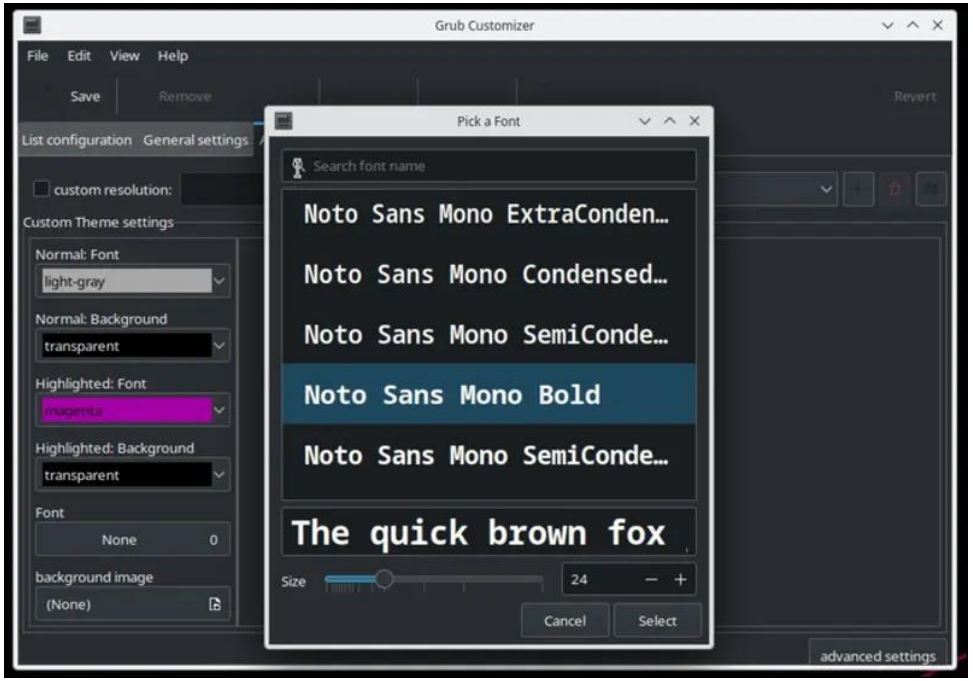
The Acer Spin 3 SP313-51N series laptops have a very nice 13.3 inch WQXGA (2560 × 1600) 16:10 IPS Touchscreen. That high resolution on a 13 inch screen makes the default GRUB menu extremely difficult to read. I had to use a magnifying glass to read it. Changing the display to 1920 × 1200 does not help until display drivers are loaded during boot. The only option to fix the tiny GRUB display is to change the font size that GRUB uses.

How to change the GRUB Font Size

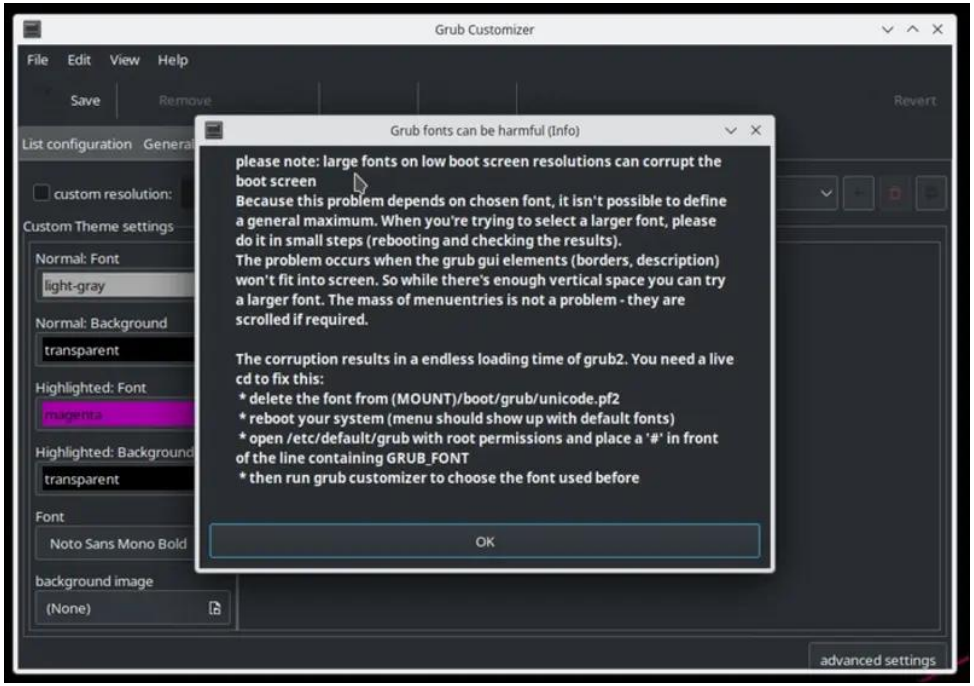
1. Open App Menu, go to Settings, and open GRUB Customizer.

2. Enter your root password.

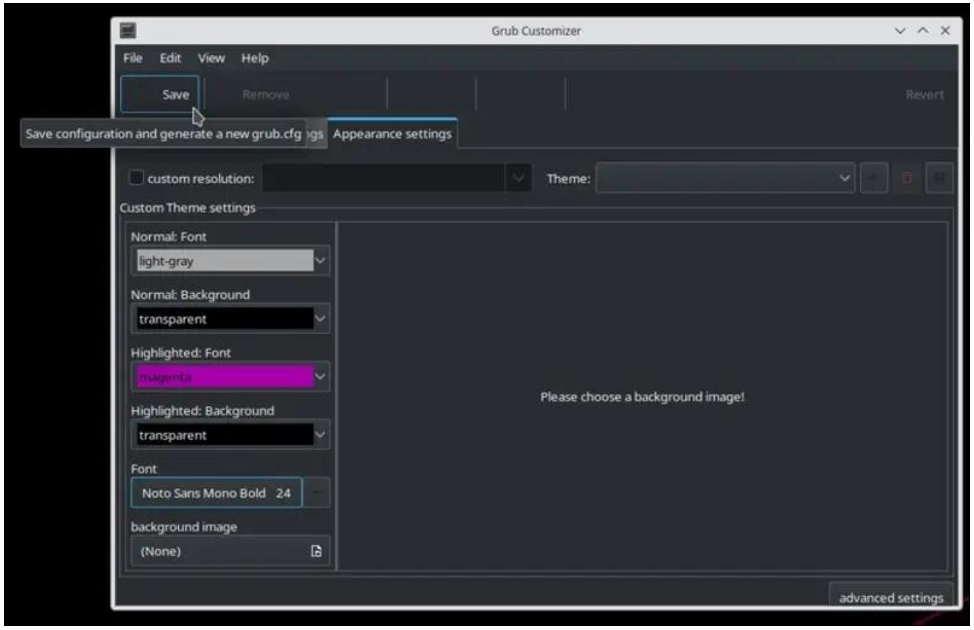
3. Click the Appearance Settings tab.



4. Use the Font Selection menu on the sidebar to pick a font that you like. I used Noto Sans Mono Bold.



5. Select the font size. I used 24 points.



6. Save your changes.

7. Close GRUB Customizer and Reboot to see your changes.

If you do not like the result, repeat the above steps and try a different font or size.

You can view the original wiki article here.

Copyright Is A Civil Liberties Nightmare

by Kit Walsh
Electronic Frontier Foundation
Reprinted under Creative Commons license

If you've got lawyers and a copyright, the law gives you tremendous power to silence speech you don't like. Copyright's statutory damages can be as high as $150,000 per work infringed, even if no actual harm is done. This makes it far too dangerous to rely on the limitations and exceptions to fair use, as you may face a financial death sentence if a court decides you got it wrong. Most would-be speakers back down in the face of such risks, no matter now legitimate their use. The Digital Millennium Copyright Act provides an incentive for platforms to remove content on your say-so, without a judge ever reviewing your papers. The special procedures and damages available to copyright owners make it one of the most appealing mechanisms for removing unwanted speech from the internet.

Copyright owners have intimidated researchers away from disclosing that their software spies on users or is full of bugs that make it unsafe. When a blockbuster entertainment product inspires people to tell their own stories by depicting themselves in the same world or costumes, a letter from the studio's lawyers will usually convince them to stay silent. And whose who sell software write their own law into End

User License Agreements and can threaten any user who disobeys them with copyright damages.

Culture has always been a conversation, not a product that is packaged up for consumption.

These are only a few of the ways that copyright is a civil liberties nightmare in the modern age, and only a few of the abuses of copyright that we fight against in court. Copyright started out as a way for European rulers to ensure that publishers remained friendly to the government, and we still see this dynamic in the cozy relationship between Hollywood and the US military and police forces. But more and more, it's been a way for private entities that are already powerful to prevent both market competition and contrary ideas from challenging their dominance.

The imbalance of power between authors and the owners of mass media is the main reason that authors only get a small share of the value they create. Copyright is at its best when it protects a creator from being beaten to market by those who own mass media channels, giving them some leverage to negotiate. With that small bit of leverage, they can get paid something rather than nothing, though the publishing deals in highly concentrated industries are famously one-sided.

But, too often, we see copyright at its worst instead, and there is no good reason for copyright law to be as broad and draconian as it is now. It lasts essentially forever, as you will probably be dead before any new works you cherished as a child will enter the public domain. It is uniquely favored by the courts as a means for controlling speech, with ordinary First Amendment considerations taking a back seat to the interests of content owners. The would-be speaker has to prove their right to speak: for example, by persuading a court that they were making a fair use. And the penalties for a court deciding your use was infringing are devastating. It's even used as a supposed justification for spying on and filtering the internet. Anyone familiar with automated copyright controls like ContentID on YouTube knows how restrictive they tend to be.

Bizarrely, copyright has grown so broad that it doesn't just bar others from reproducing a work or adapting it into another medium such as film, it even prevents making original stories with a character or setting "owned" by the copyright owner. For the vast majority of our history, humans have built on and retold one another's stories. Culture has always been a conversation, not a product that is packaged up for consumption.

The same is true for innovation, with a boom in software technology coming before copyright was applied to software. And, thanks to free software licenses that remove the default, restrictive behavior of copyright, we have communities of scrappy innovators building tools that we all rely upon for a functioning internet. When the people who depend upon a technology have a say in creating it and have the option to build their own to suit their needs, we're much more likely to get technology that serves our interests and respects our privacy and autonomy. That's far superior to technology that comes into our homes as an agent of its creators, seeking to exploit us for advertising data, or limit our choices of apps and hardware to serve another's profit motive.

EFF has been at the vanguard for decades, fighting back against copyright overreach in the digital world. More than ever, people need to be able to tell their stories, criticize the powerful and the status quo, and to communicate with technologies that aren't censored by overzealous copyright bots.

Screenshot Showcase

Posted by Meemaw, on February 22, 2025, running Xfce.

GIMP Tutorial: Using The Cage Transformation Tool

by Meemaw

Browsing through the tutorials, I saw one about the Cage Transformation tool in GIMP. It's a little different because it lets you bend things around any way you want. It doesn't keep things in perspective, so I hadn't used it much. Usually, if I want to transform something, I'm still concerned about perspective and straight lines. (This tutorial is one that comes to mind.)

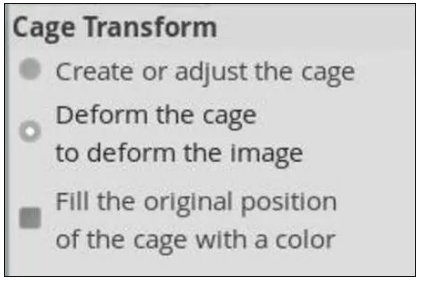
Using the Cage Transformation tool is relatively easy, but it's also easy to make a mess. However, that may be what you're aiming for. Let's get started!

Open GIMP and import a photo you want to transform. The tutorial I saw (one of many) used a vehicle, and changed the shape of it, so I loaded this photo into GIMP. This vehicle was in a parade in my town several years ago. I'm going to transform the car.

The very FIRST thing you want to do is to duplicate your layer. Next, select the Cage Transformation tool. Your cursor will change as shown on the right below:

Click around the object you want to transform, making a path all the way around it with nodes every so often, so the nodes can be manipulated. When you get all the way around, close the path by clicking on the first node.

While you're drawing your path, the tool option (top, right) under your toolbox will have the top option selected: "Create or adjust the cage". When you close your path/cage, the choice will change to "Deform the cage to deform the image". **DO NOT** press Enter yet.



Now you can start moving the nodes. When you move one, and release your mouse button, you'll see that a portion of your photo will move to a different position. This is where it's up to you what's done. The first time I did this, I deformed the front of the car, and the second time, I deformed the back.

Push these nodes around however you want. When you have it the way you want it, press **Enter**, and your deform will be done, and your nodes will disappear. You'll notice that the area between your object and your path has been deformed as well. This isn't hard to fix, but it's a little "fiddly".

See the background behind the car? We'll fix it. Go to the Layers dialog, right-click on the layer you're working on, and choose **Add Alpha Channel**. This will give your layer transparency, and we can erase the parts that are deformed. When we erase, the bottom layer will show through, and it won't be deformed.

If you made something smaller, you may also have to fill in, carefully. I didn't do the shadow under the car.

My finished product:

Like I said, my first attempt deformed the front of the car:

I hope you had fun with this one!

GIMP 3.0 is coming! Release Candidate 3 was released on February 10th, and I hope the final is released soon!

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.

When Platforms & The Government Unite, Remember What's Private & What Isn't

by Thorin Klosowski and Matthew Guariglia
Electronic Frontier Foundation

For years now, there has been some concern about the coziness between technology companies and the government. Whether a company complies with casual government requests for data, requires a warrant, or even fights overly-broad warrants has been a canary in the digital coal mine during an era where companies may know more about you than your best friends and families. For example, in 2022, law enforcement served a warrant to Facebook for the messages of a 17-year-old girl — messages that were later used as evidence in a criminal trial that the teenager had received an abortion. In 2023, after a four-year wait since announcing its plans, Facebook encrypted its messaging system so that the company no longer had access to the content of those communications.

The privacy of messages and the relationship between companies and the government have real-world consequences. That is why a new era of symbiosis between big tech companies and the U.S. government bodes poorly for both, our hopes that companies will be critical of requests for data, and any chance of tech regulations and consumer privacy legislation. But, this chumminess should also come with a heightened awareness for users: as companies and the government become more entwined through CEO friendships, bureaucratic entanglements, and ideological harmony, we should all be asking what online data is private and what is sitting on a company's servers and accessible to corporate leadership at the drop of hat.

Over many years, EFF has been pushing for users to switch to platforms that understand the value of encrypting data. We have also been pushing platforms to make end-to-end encryption for online communications and for your stored sensitive data the norm. This type of encryption helps ensure that a conversation is private between you and the recipient, and not accessible to the platform that runs it or any other third-parties. Thanks to the combined efforts of our organization and dozens of other concerned groups, tech users, and public officials, we now have a lot of options for applications and platforms that take our privacy more seriously than in previous generations. But, in light of recent political developments, it's time for a refresher course: which platforms and applications have encrypted DMs, and which have access to your sensitive personal communications.

The existence of what a platform calls "end-to-end encryption" is not foolproof. It may be poorly implemented, lack widespread adoption to attract the attention of security researchers, lack the funding to pay for security audits, or use a less well-established encryption protocol that doesn't have much public scrutiny. It also can't protect against other sorts of threats, like someone gaining access to your device or screenshotting a conversation. Being caught using certain apps can itself be dangerous in some cases. And it takes more than just a basic implementation to resist a targeted active attack, as opposed to later collection. But it's still the best way we currently have to ensure our digital conversations are as private as possible. And more than anything, it needs to be something you and the people you speak with will actually use, so features can be an important consideration.

No platform provides a perfect mix of security features for everyone, but understanding the options can help you start figuring out the right choices. When it comes to popular social media platforms, Facebook Messenger uses end-to-end encryption on private chats by default (this feature is optional in group chats on Messenger, and on some of the company's other offerings, like Instagram). Other companies, like X, offer

optional end-to-end encryption, with caveats, such as only being available to users who pay for verification. Then there's platforms like Snapchat, which have given talks about their end-to-end encryption in the past, but don't provide further details about its current implementations. Other platforms, like Bluesky, Mastodon, and TikTok, do not offer end-to-end encryption in direct messages, which means those conversations could be accessible to the companies that run the platforms or made available to law enforcement upon request.

As for apps more specifically designed around chat, there are more examples. Signal offers end-to-end encryption for text messages and voice calls by default with no extra setup on your part, and collects less metadata than other options. Metadata can reveal information such as who you are talking with and when, or your location, which in some cases may be all law enforcement needs. WhatsApp is also end-to-end encrypted. Apple's Messages app is end-to-end encrypted, but only if everyone in the chat has an iPhone (blue bubbles). The same goes for Google Messages, which is end-to-end encrypted as long as everyone has set it up properly, which sometimes happens automatically.

Of course, we have a number of other communication tools at our disposal, like Zoom, Slack, Discord, Telegram, and more. Here, things continue to get complicated, with end-to-end encryption being an optional feature sometimes, like on Zoom or Telegram; available only for specific types of communication, like video and voice calls on Discord but not text conversations; or not being available at all, like with Slack. Many other options exist with varying feature-sets, so it's always worth doing some research if you find something new. This does not mean you need to avoid these tools entirely, but knowing that your chats may be available to the platform, law enforcement, or an administrator is an important thing to consider when choosing what to say and when to say it.

And for high-risk users, the story becomes even more complicated. Even on an encrypted platform, users can be subject to targeted machine-in-the middle attacks (also known as man-in-the middle attacks) unless everyone verifies each other's keys. Most encrypted apps will let you do this manually, but some have started to implement automatic key verification, which is a security win. And encryption doesn't matter if message backups are uploaded to the company's servers unencrypted, so it's important to either choose to not backup messages, or carefully set up encrypted backups on platforms that allow it. This is all before getting into the intricacies of how apps handle deleted and disappearing messages, or whether there's a risk of being found with an encrypted app in the first place.

CEOs are not the beginning and the end of a company's culture and concerns—but we should take their commitments and signaled priorities seriously. At a time when some companies may be cozying up to the parts of government with the power to surveil and marginalize, it might be an important choice to move our data and sensitive communications to different platforms. After all, even if you are not at specific risk of being targeted by the government, your removed participation on a platform sends a clear political message about what you value in a company.

PCLinuxOS Recipe Corner Bonus

Chocolate-Dipped Ice Cream Tacos

Serves: 8

A real treat that both the young and old will enjoy!

INGREDIENTS:

Taco Shells

2 large eggs
1/2 cup sugar
1/4 cup milk
1 teaspoon vanilla extract
1/4 cup unsalted butter, 1/4 stick, melted
1/2 cup all purpose flour
1 tablespoon cocoa powder

Magic Shell

18 oz good-quality chocolate, finely chopped
1/4 cup coconut oil, melted

Assembly

4 cups vanilla ice cream, softened
1 cup salted peanut, crushed

DIRECTIONS:

Make the taco shells: in a medium bowl, whisk together the eggs and sugar until combined.

Add the milk, vanilla, and butter, and whisk until fully incorporated.

Sift in the flour and cocoa powder. Whisk until smooth.

Heat a small non-stick pan over medium-low heat, then add ⅓ cup (95 g) of batter at a time and tilt the pan to spread the batter evenly like a crepe.

Cook until bubbles appear on the surface and the batter is set, about 6-8 minutes. Flip the taco shell and cook on the other side for another 3-4 minutes, until cooked through.

If desired, remove the taco shell from the pan and place on a grated cooling rack while still hot. Place a sheet of parchment over the shell and press into the rack, allowing the grate marks to set into the shell. Rotate the shell 90 degrees and press the cone into the grates again for a waffled look. Or, skip to the next step.

Place the taco shells between the cups of an inverted muffin tin to form their shape. Let set for about 10 minutes, then freeze for 20 minutes to harden.

Make the magic shell: combine the chocolate and coconut oil in a medium bowl and microwave for 2 minutes, stirring every 30 seconds until melted and shiny.

Remove the taco shells from the freezer and use a spoon to coat the inside of each taco shell with melted magic shell. Return to the freezer for 20 minutes, until the magic shell hardens. Reserve the leftover magic shell.

Add the ice cream to a piping bag fitted with a round tip or a zip-top bag with the corner cut off.

Remove the shells from the freezer and pipe in the ice cream, filling the tacos. Smooth out the tops with a knife or rubber spatula. Freeze for 2 hours.

Microwave the reserved magic shell, if needed, to re-melt. Remove the tacos from the freezer and dip the tops of each taco in the magic shell, then immediately sprinkle with the crushed peanuts.

Serve immediately or return to the freezer until ready to eat.

Enjoy!

NUTRITION:

Calories: 884 Carbs: 83g Sodium: 207mg
Fiber: 5g Protein: 16g

Screenshot Showcase

Posted by sam2fish, on February 4, 2025, running KDE.

PCLinuxOS Puzzled Partitions

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

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.

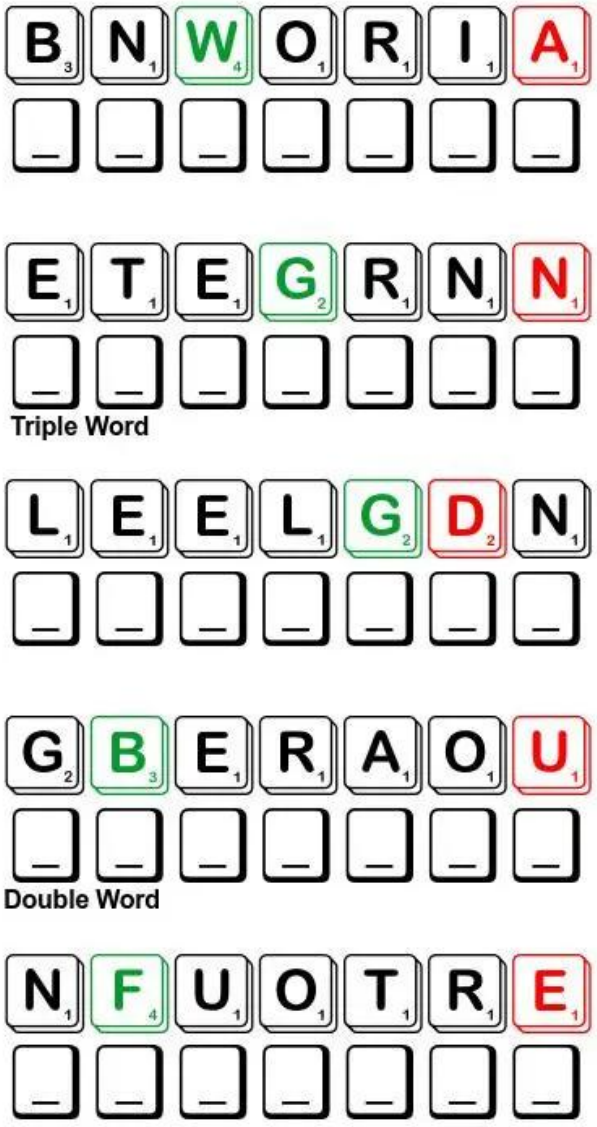
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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 237, average score 166.

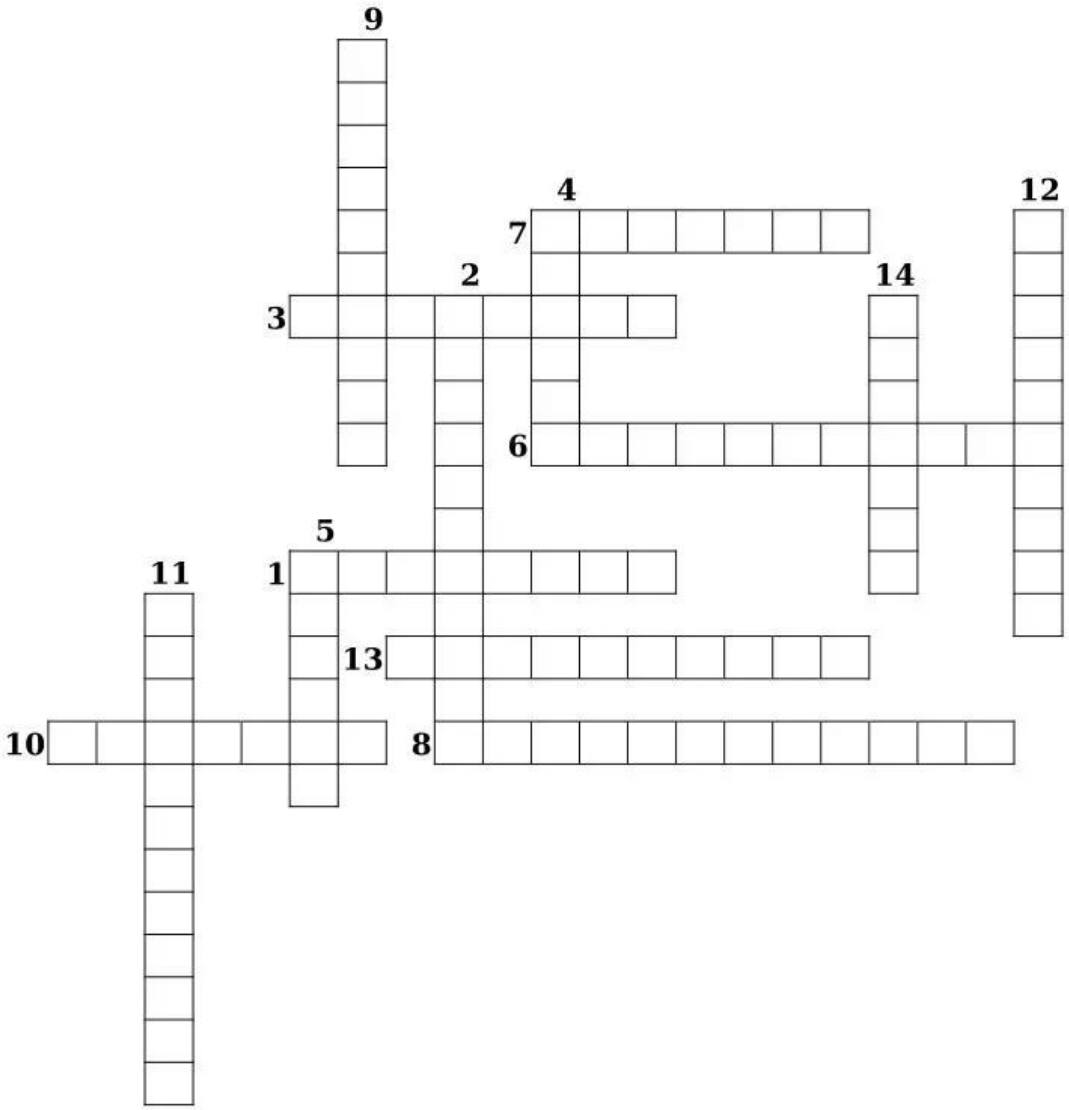
March 2025 Word Find
St. Patricks Day

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

BAGPIPE
BLARNEY STONE
BROGUE
DONNYBROOK
EMERALD ISLE
FORTUNE
FOUR-LEAF CLOVER
GOOD LUCK
GREEN
LEGEND
LEPRECHAUN
LIMERICK
LUCK OF THE IRISH
MAGICAL
MARCH
MISCHIEVOUS
POT OF GOLD
POTATO
RAINBOW
SAINT PATRICK
SEVENTEENTH
SHAMROCK
SHILLELAGH
WALKING STICK
WEARING OF THE GREEN

Download Puzzle Solutions Here

March 2025 Crossword
St. Patricks Day



1. A humorous, often nonsensical, and sometimes risqé poem.
2. Slightly bad or annoying, especially in a playful way.
3. A four-leaf clover, used as a symbol of Ireland.
4. A strong dialectal accent, especially strong Irish or Scottish.
5. An unverified story handed down from earlier times, especially one popularly believed to be historical.
6. A nickname for Ireland.
7. A musical instrument having an inflatable bag, played using a mouthpiece & keys.
8. Apostle and patron saint of Ireland.
9. A small mischievous elf or spirit in Irish folklore.
10. Success, especially when at least partially resulting from luck.
11. A block built into Blarney Castle, said to bring you good luck if you kiss it.
12. A thick, heavy, wooden stick, used as a club or walking stick.
13. A chaotic brawl or a heated argument.
14. Enchanting; bewitching.

Download Puzzle Solutions Here

Mixed-Up-Meme Scrambler

BIBAR

DEYNE

SHOIMD

MELVUL

When the woman pilot got married,
her friends said she .....

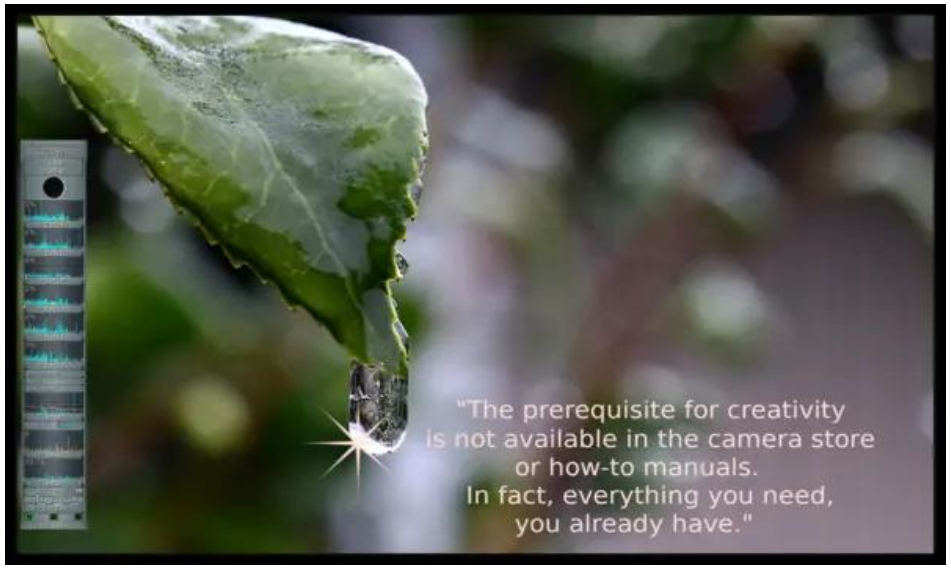
" _ _ _ _ _ _ " _ _ _

Download Puzzle Solutions Here

More Screenshot Showcase

Posted by supahglue, on February 1, 2025, running KDE.

Posted by tbs, on February 23, 2025, running KDE.



Posted by The_CrankyZombie, on January 31, 2025, running KDE.

Posted by weirdwolf, on February 5, 2025, running LXDE.