# The PCLinuxOS magazine

Volume 230

March, 2026

# In This Issue...




The PCLinuxOS magazine

The PCLinuxOS name, logo and colors are the trademark of Texstar. **The PCLinuxOS Magazine** is a monthly online publication containing PCLinuxOS-related materials. It is published primarily for members of the PCLinuxOS community. The magazine staff is comprised of volunteers from the PCLinuxOS community.

Visit us online at https://pclosmag.com.

This release was made possible by the following volunteers:
**Chief Editor**: Paul Arnote (parnote)
**Assistant Editor**: Meemaw
**Artwork**: Paul Arnote, Meemaw
**PDF Layout**: Paul Arnote, Meemaw
**HTML Layout**: tbs, horusfalcon

**Staff**:
YouCanToo David Pardue
Alessandro Ebersol

**Contributors**:
ramchu

# From The Chief Editor's Desk

I guess you can say that “we” are a “cat family.”

Up until recently, we had eight of those furry little buggers running around here.

How did we get to the point that we had eight cats? Well, there’s a number of factors involved. First, I guess you could say I married a “crazy cat lady.” Second, I also have a fondness for cats. They are more self-sufficient than dogs. You can go away for an evening or two, and cats will do just fine on their own. Third, we live just three doors down from a city park. As sad and unfortunate as reality might be, it’s not uncommon for people to drop off their unwanted pets at the park.

*Mom and dad were honored for our work with Scouts at a recent awards ceremony.*

Now how they find their way to our door, sometimes I feel like we must have a neon sign posted in front of our house that only cats can see. It seems like every cat dropped off at the park by their irresponsible owners finds their way to our door.

I guess you could say that there’s a fourth factor involved. That is the ability to “just say no.” And, for a long time, that was the case. It seems that “eight” was the magic number for us to learn to say “no more.”

Every single one of the cats we have were strays, most of them dropped off at the local park. They all came to us as strays.

But recently, we had to deal with losing three of our cats. First, Smokie died. Then, my son’s cat, Pixie (a.k.a. CiCi, since my son couldn’t say “Pixie” when he was little … it came out as CiCi, and the name just stuck) passed away. Then, our “outdoor cat,” Callie, passed away. All of them lived long, long lives, and died from (basically) old age. They all lived a much longer life with us than they ever would have had we not taken them in.

Since they were all strays, we were never quite sure exactly how old any of them are or were. Smokie was at least 20 years old. Pixie/CiCi was over 20 years old (we’re guessing that he was close to 25 years old). Callie had to be close to 20 years old, if not more.

Cats are a LOT like people. They each have their own unique personalities, their own likes and dislikes, their own quirks. Even if you blindfold me, I can tell you the name of any of our cats, just by their voices. But anyone who has had cats already knows this.

Don’t get me wrong. I like dogs, too. But a dog just hasn’t fit into our lives the way that the cats have. And, we are “animal” people. My nine year old daughter has two leopard geckos. My son has had pet tarantulas on two separate occasions. Plus, we have nine hens in our “backyard flock,” and six new baby chicks growing up in the brooder in our dining room.

So, maybe it's more accurate to say that we are "animal" people. No judgments here, though. I know some people just aren't animal people. For others, animals just don't fit into their lives. But, there are also a LOT of "animal" people in our midst.

**********

This month's cover image was created by Bing Image Creator, and celebrates Tux as the great magician, Harry Houdini. Houdini's birthday is March 24, and he was born in 1874. He tragically died in 1926. You can read more about his life here.

**********

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


# ICYMI: Massive Unsecured Database Exposes 149 Million Logins

**by Paul Arnote (parnote)**

*Image by Jan from Pixabay*

**Another wave of malicious browser extensions capable of tracking user activity and compromising privacy have been found across Chrome, Firefox, and Edge, some of which may have been active for up to five years**, according to an article from Lifehacker. The campaign, known as GhostPoster, was identified by Koi Security in December and included 17 Firefox add-ons designed to monitor users' browsing activity. Threat actors planted malicious JavaScript code in the extension's PNG logo, which served as a malware loader to retrieve the main payload from a remote server. Researchers at LayerX have found an additional 17 malicious extensions across multiple browsers that have collectively been installed more than 840,000 times.

**YouTube is taking a sledgehammer to the low-grade AI garbage cluttering up your feed**, according to an article by eWeek. In his annual look-ahead letter, YouTube CEO Neal Mohan laid out a year of big bets, including AI tools alongside a crackdown on what the internet has nicknamed "AI slop." This comes after announcing that more than a million channels used its AI creation tools every day last December. The irony of the war on "slop" is that YouTube is actually giving creators more AI tools, not fewer. Later this year, creators will be able to generate Shorts using their own AI-generated likeness. The platform is also testing ways for people to build games and music using nothing but text prompts. But he admits the tech brings serious problems. "It's becoming harder to detect what's real and what's AI-generated," Mohan wrote in the official company letter. "This is particularly critical when it comes to deepfakes."

It's not just you. Google Search has become significantly worse in recent years. In the past, you only had to watch out for low-quality content filled with SEO-bait keywords. Today, you have to be wary of AI-generated garbage, misinformation, and a generally worse UI. **Still, it's not impossible to find good search results on Google**, according to an article from Lifehacker. The author has found a number of tricks that have helped reduce the number of low-quality entries Google returns for his searches. Here are 10 such tips everyone should know about before their next search.

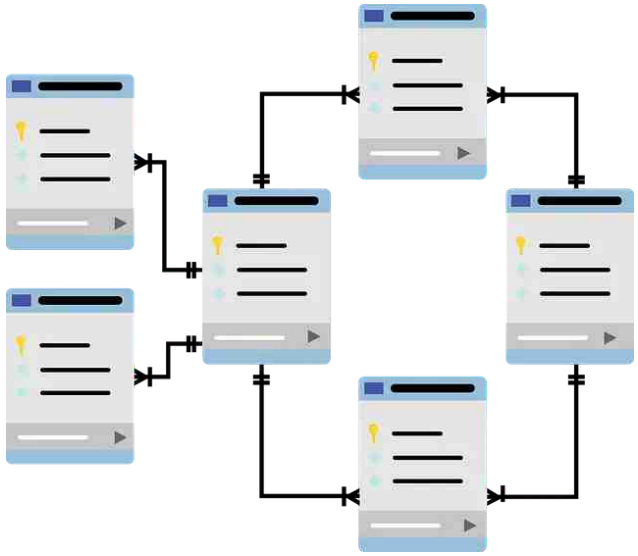


*Image by mcmurryjulie from Pixabay*

A massive unsecured database exposed 149 million logins, raising concerns over infostealer malware and credential theft. Jeremiah Fowler, a veteran security researcher, **recently stumbled upon 149,404,754 unique logins and passwords, totaling about 96GB of raw data. There was no encryption… and it didn't even have a password,** according to an article from TechRepublic. Sharing his findings with ExpressVPN, Fowler noted, "The publicly exposed database was not password-protected or encrypted." The collection was so large and detailed that it wasn't just a list of names; it included emails, usernames, passwords, and the

specific website links needed to log into the accounts.

**Crunchbase confirmed a data breach after the cybercriminal group ShinyHunters claimed to steal over 2 million personal records from its systems**, according to an article from SecurityAffairs. The group leaked a 402 MB compressed archive on their website due to a failed extortion attempt. The company states that operations weren't affected and that the security breach is now contained. Crunchbase notified federal authorities and is investigating the incident with the help of external experts. The company is reviewing the exposed data to determine if any legal notifications are needed.

**Microsoft is under scrutiny after it emerged that the company shared encryption keys with US law enforcement, an uncommon move that has alarmed privacy experts and reignited the debate over who truly controls encrypted data**, according to an article from TechRepublic. According to Forbes staffer Thomas Brewster, Microsoft provided the FBI with BitLocker recovery keys that allowed investigators to unlock data on three encrypted laptops. The request came through a valid search warrant issued in a federal investigation in Guam into alleged fraud in the island's COVID-19 unemployment assistance program. The laptops were protected by BitLocker, Microsoft's full-disk encryption software that is enabled by default on many modern Windows PCs. While BitLocker is designed to keep data safe from unauthorized access, the case shows that protection depends heavily on where the recovery key is stored.

*Image by OpenClipart-Vectors from Pixabay*

**Early hominins in Europe were creating tools from raw materials hundreds of thousands of years before Homo sapiens arrived there, two new studies indicate, pushing back the established time for such activity**, according to an article from the New York Times. The evidence includes a 500,000-year-old hammer made of elephant or mammoth bone, excavated in southern England, and 430,000-year-old wooden tools found in southern Greece — the earliest wooden tools on record. The findings suggest that early humans possessed sophisticated technological skills, the researchers said. Katerina Harvati, a paleoanthropologist at the University of Tübingen in Germany and a lead author of the wooden-tool paper, which was published on Monday in the journal PNAS, said the discoveries provided insight into the prehistoric origins of human intelligence. Silvia Bello, a paleoanthropologist at London's Natural History Museum and an author on the elephant-bone study, which was published last week in Science Advances, concurred.

**Tech companies are getting increasingly pushy with their large language models — prominent buttons for these AI features coat every surface designers can think of, including in three of the most prominent browsers: Chrome, Edge, and Firefox**, according to an article from Lifehacker. If you want these AI features to go away, and stay away, there's a script for that. JustTheBrowser is a free and open source tool from developer and tech blogger Corbin Davenport that removes AI features, telemetry data reporting, sponsored content, product integrations, and other annoyances from Chrome, Firefox, and Microsoft Edge. Basically, you can run this once and never think about these features again. To get started, head to the JustTheBrowser homepage. There are scripts to copy (which I'm not going to include here in case they change in the future).

**There are reports that a legitimate Microsoft email address — which Microsoft explicitly says customers should add to their allow list — is delivering scam spam**, according to an article from Ars Technica. The emails originate from no-reply-powerbi@microsoft.com, an address tied to Power BI. The Microsoft platform provides analytics and business intelligence from various sources that can be integrated into a single dashboard. Microsoft documentation says that the address is used to send subscription emails to mail-enabled security groups. To prevent spam filters from

blocking the address, the company advises users to add it to allow lists.

*Image by Shakti Shekhawat from Pixabay*

**Panera Bread has been named by the cybercrime group ShinyHunters as the latest victim in a large-scale stolen credentials incident**, according to an article from TechRepublic. This raises fresh concerns about the security of single sign-on systems and the growing effectiveness of social engineering attacks targeting major consumer brands. The group claims it obtained sensitive customer data linked to Panera Bread and has listed the company on its data leak site alongside other high-profile organizations. While Panera Bread has not publicly confirmed the breach, the allegations point to the exposure of millions of customer records and highlight a wider campaign that security researchers say is affecting companies across multiple sectors. The info was shared on Daily Dark Web, where approximately 14 million Panera Bread customer records were taken during the intrusion. The dataset allegedly includes names, email addresses, postal addresses, phone numbers, and account-related details. The group claims the stolen information amounts to roughly 760 MB of compressed data. If accurate, the scale of the alleged breach would place it among the larger consumer data exposures reported in recent months, particularly within the food and retail sector.

**Mozilla announced that new AI controls are coming to Firefox, starting with Firefox 148**, according to an article from Lifehacker. This version, which drops Feb. 24, sports a brand-new AI controls section in the settings panel on the desktop browser. (You'll find it in the between "Sync" and "AI controls.") From here, you'll be able to block all current and future AI features, and cherry pick which features you want to use — if any. If you want absolutely nothing to do with AI when browsing the web with Firefox, you can use the "Block AI enhancements" toggle. Once activated, not only will these features not appear, but Firefox will block any pop-ups or alerts pushing you to try existing or future AI features.

**Jupiter is smaller and flatter than scientists previously thought, new measurements of the gas giant reveal**, according to an article from LiveScience. Researchers used radio data from the Juno spacecraft to refine measurements of the solar system's largest planet. Although the differences between the current and previous measurements are small, they are improving models of Jupiter's interior and of other gas giants like it outside the solar system, the team reported Feb. 2 in the journal Nature Astronomy. "Textbooks will need to be updated," study co-author Yohai Kaspi, a planetary scientist at the Weizmann Institute of Science in Israel, said in a statement. "The size of Jupiter hasn't changed, of course, but the way we measure it has."

Malwarebytes

**Malwarebytes has joined the ChatGPT app store, which means you can get some expert help when investigating web links, emails, text messages, domains, and phone numbers you think might be suspicious**, according to an article from Lifehacker. The app is free to use for everyone, whether or not they're signed up to a paid ChatGPT subscription, and you can enable the tool via the ChatGPT app store or by entering the prompt "Malwarebytes, is this a scam?" Once you've used the app for the first time, you can access it again via the + (plus) button on the prompt box.

**Photo-sharing platform Flickr is notifying users of a potential data breach after a vulnerability at a third-party email service provider exposed their real names, email addresses, IP addresses, and account activity**, according to an article from BleepingComputer. Founded in 2004, Flickr is one of the world's largest photography communities and sharing sites, hosting over 28 billion photos and videos. The company says it has 35 million monthly users and 800 million monthly page views. Flickr did not disclose which third-party provider was involved or how many users were potentially affected by this incident. A Flickr spokesperson was not immediately available for comment when contacted by BleepingComputer

for more details. The company said that it shut down access to the affected system within hours after being informed of the security flaw on February 5. While the vulnerability "may have" provided access to some member information, Flickr said that passwords and payment card numbers were not compromised in the incident.

**Google announced two new ways for users to remove their sensitive information from the web Tuesday morning—or, at least, remove that data from Google Search. The first lets users request that Google remove sensitive government ID information from Search, while the second gives users new tools to request the same for non-consensual explicit images**, according to an article from Lifehacker. Google is updating its existing "Results about you" tool, which helps users scour the internet for their personal information. Before today, this tool could already locate data points like your name, phone number, email addresses, and home addresses. Following the update, you can now find and request the deletion of search results containing highly sensitive information, including your driver's license, passport, or Social Security number.


*Image by Mohamed Hassan from Pixabay*

**Researchers at the University of Wisconsin-Madison discovered that a concerning number of browser extensions can access sensitive information that you enter into websites. Think passwords, credit card info, and Social Security numbers**, according to an article from Lifehacker. The team behind the discovery says they weren't out looking to break a security story. Instead, they were "messing around with login pages," specifically Google login pages, when they found that the sites' HTML source code could see the passwords they entered in plain text. They turned their sights onto other websites—more than 7,000, reportedly—and found that about 15% of them were also storing sensitive information in plain text. That's over 1,000 websites exposing important data.

**Releasing male *Aedes aegypti* mosquitoes into the wild that were infected with the sterility-inducing bacteria Wolbachia pipientis cut dengue infection risk more than 70% in people, according to a cluster-randomized trial in Singapore**, says an article from MedPage Today. In urban locations where wolbachia-infected male mosquitoes were introduced, the percentage of residents who tested positive for dengue infection at 6 months or more after the intervention was 6% (354 of 5,722 tests) compared with 21% (1,519 of 7,080 tests) in urban locations where the infected male mosquitoes weren't introduced, reported Lee Ching Ng, PhD, of the National Environment Agency in Singapore, and colleagues. The intervention's protective efficacy after 3 months was 71%, reaching 72% at 6 months and settling at 71% 12 months and later, the researchers detailed in the New England Journal of Medicine.

Threat actors don't have to work that hard to obtain sophisticated malware to deploy against unsuspecting targets. **A new spyware platform known as ZeroDayRAT is reportedly being sold on Telegram, complete with customer support and updates**, according to an article from Lifehacker. According to mobile security company iVerify, this aggressive spyware grants full remote control over devices running Android 15 through 16 and iOS versions up to iOS 26. Once deployed, it allows everything from user profiling and location tracking to live surveillance and financial theft.

*Image by Mohamed Hassan from Pixabay*

It's tempting to think that an LLM chatbot can answer any question you pose, including those about your health. After all, chatbots have been trained on plenty of medical information, and can regurgitate it if given the right prompts. But that doesn't mean they will give you accurate medical advice, and **a new study shows how easily AI's supposed expertise breaks down**, according to an article from Lifehacker. In short, they are even worse at it than I thought. In the study, researchers first quizzed several chatbots about medical information. In these carefully conducted tests, ChatGPT-4o, Llama 3, and Command R+ correctly diagnosed medical scenarios an impressive 94% of the time—though they were able to recommend the right treatment a much less impressive 56% of the time.

**Google confirms Quick Share's AirDrop-style sharing is expanding beyond Pixel to more Android devices in 2026, making file sharing far easier**, according to an article from TechRepublic. The Pixel-only phase is ending. Quick Share's AirDrop interoperability is on its way to a much bigger slice of Android. Google has now confirmed it's expanding AirDrop-style sharing beyond its own Pixel phones to a much wider range of Android devices in 2026. That move could finally make fast, local file sharing feel less like a platform privilege and more like a standard feature for Android users everywhere.

**Getting older might seem like a slow, gradual process – but research suggests that this is not always the case**, according to an article from ScienceAlert. In fact, if you wake up one morning, look in the mirror, and wonder if your aging somehow accelerated, you might not be imagining things. According to a 2024 study into the molecular changes associated with aging, humans experience two abrupt lurches forward, one at the average age of 44 and the other at around age 60.

*Image by Shelley Evans from Pixabay*

Raise your hand if you didn't see THIS coming. AI-powered browser extensions continue to be a popular vector for threat actors looking to harvest user information. **Researchers at security firm LayerX have analyzed multiple campaigns in recent months involving malicious browser extensions**, including the widespread GhostPoster scheme targeting Chrome, Firefox, and Edge. In the latest one — dubbed AiFrame — threat actors have pushed approximately 30 Chrome add-ons that impersonate well-known AI assistants, including Claude, ChatGPT, Gemini, Grok, and "AI Gmail." Collectively, these fakes have more

***A magazine just isn't a magazine without articles to fill the pages. If you have article ideas, or if you would like to contribute articles to the PCLinuxOS Magazine, send an email to: pclinuxos.mag@gmail.com We are interested in general articles about Linux, and (of course), articles specific to PCLinuxOS.***

than 300,000 installs, according to an article from Lifehacker.

**In a laboratory at Tsinghua University in China, researchers have successfully tackled one of the most persistent limitations in 3D printing**, according to an article from TechSpot. They have developed a system that can produce intricate, millimeter-scale objects almost instantaneously – no layering, no waiting, and no compromise between fine detail and rapid output. The technique is called Digital Incoherent Synthesis of Holographic light fields (DISH). Instead of assembling materials layer by layer, DISH projects a three-dimensional holographic light field directly into a resin volume, solidifying the entire object at once.

It's one of the most instantly recognizable scenes in cinematic history: Luke Skywalker gazes at a double sunset to the haunting melody of a mournful French horn. And while "Star Wars" may take place in a galaxy far, far away, planets orbiting binary stars actually do exist in the Milky Way. **Yet mysteriously, there are not as many as scientists expect — and new research might explain why**, according to an article from Space.com. Of the thousands of single-star systems in our galaxy, around 10% are known to have planets. Scientists thus expected about 10% of the 3,000 known binary star systems in our galaxy to have them, too. But of the more than 6,000 confirmed exoplanets in the Milky Way, just 14 confirmed planets have been found around pairs of stars. Researchers from the University of California, Berkeley, and the American University of Beirut suggest the culprit might be Albert Einstein's theory of general relativity.

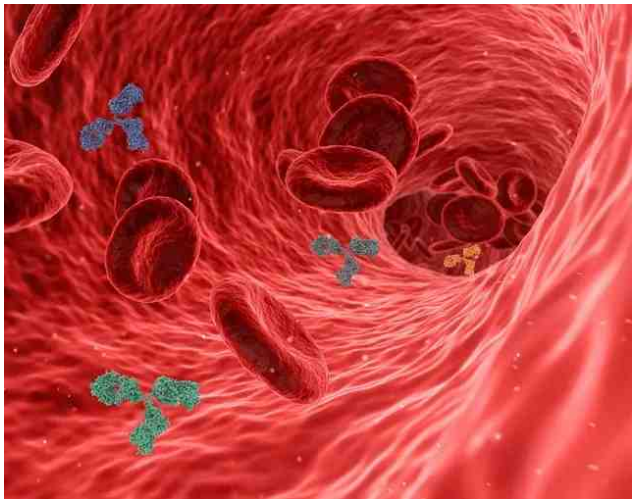


*Image by swiftsciencewriting from Pixabay*

**After years of work, scientists have solved the mystery of an unusual side effect that impacted some recipients of the Oxford/ AstraZeneca and Johnson & Johnson COVID-19 vaccines**, according to an article from IFL Science. Most importantly, the discovery could help vaccine developers to produce safer vaccines based on the same technology, preventing the same issues occurring in the future. Most of the COVID vaccines still in use today are mRNA vaccines, but some of the ones rolled out earlier in the pandemic, notably from Oxford/AstraZeneca in the UK and Johnson & Johnson in the US, were different. These were adenovirus vector vaccines, which use a harmless-to-humans carrier virus (in this case, an adenovirus) to transport part of the virus they're actually trying to vaccinate against. The reason why these COVID vaccines were able to be developed so quickly was because this technology was not new – the developers of the Oxford/AstraZeneca vaccine, for instance, had already been trialing an adenovirus vector vaccine against MERS, another coronavirus, when the pandemic hit. They were very effective, and alongside the mRNA vaccines from Pfizer and Moderna were cornerstones of the early response to the pandemic, helping to turn the tide of infections, save lives, and allow restrictions to be lifted. But no medical intervention is completely risk-free, and it quickly became apparent that a very rare side effect was impacting some of those receiving the adenovirus vaccines.

**Astronomers recently searched the gas cloud of a yet-unborn star for a chemical that may seed future planets with the basic ingredients for life**, according to an article from Space.com. Astronomer Yuxin Lin and colleagues found an organic molecule called methanimine scattered throughout a dense clump of gas and dust 554 light-years away. The cloud, called L1544 and found within the Taurus Molecular Cloud, will eventually become a star with a system of planets, and if Lin and colleagues are right, those exoplanets may form with a "starter kit" of organic molecules like methanimine — courtesy of chemical reactions that are going on right now in the cold, dormant molecular cloud. Astronomers have spotted methanimine in a surprising range of places in the universe, from very hot and turbulent places like the cores of newborn stars to frigid grains of ice drifting through interstellar space. One of the most interesting places methanimine has turned up is what astronomers call a pre-stellar core: a dense knot of gas and dust, poised on the brink of

collapsing under its own gravity to form a newborn star. Think of a pre-stellar core — like L1544, located 554 light years away — as all the ingredients for a star system, with some assembly required.

**Researchers have resolved a 50-year-old scientific mystery by identifying the molecular mechanism that allows tissues to regenerate after severe damage. The discovery could help guide future treatments aimed at reducing the risk of cancer returning**, according to an article from SciTechDaily. Many tissues in the body, including the skin and other epithelial layers that line organs, have a remarkable ability to recover after severe damage. Instead of simply breaking down, they can trigger a surge of new cell growth that restores lost tissue. New research from the Weizmann Institute of Science, published in *Nature Communications*, sheds light on how this regeneration occurs. The study shows that caspases, enzymes best known for driving cell death, can also help certain cells survive and support tissue repair. By doing so, these cells enable damaged tissue not only to regrow but, in some cases, to become more resistant to future stress. The researchers also found a potential downside to this process. The same survival mechanism may be exploited by cancer cells, helping tumors return in a more aggressive and treatment-resistant form. Understanding this pathway could therefore inform new strategies to improve wound healing and reduce the risk of cancer relapse.


**Google has issued a patch for a high-severity flaw that has been actively exploited in the wild—the first Chrome zero-day in 2026**, according to an article from Lifehacker. The latest flaw, catalogued as CVE-2026-2441, is a use-after-free vulnerability in CSSFontFeatureValuesMap, Chrome's CSS font feature implementation. A use-after-free vulnerability is a flaw in which an application attempts to use memory after it has been released back to the system. This type of bug allows attackers to execute code, escalate privileges, cause app or system crashes, and leak sensitive data. CVE-2026-2441 would allow "a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page." Essentially, this means malicious HTML content could run code inside a Chrome tab, extension, or plugin. As Malwarebytes explains, this is dangerous because attackers can see or modify whatever the isolated browser tab (sandbox) can access, allowing actions like credential harvesting and traffic rerouting—even if it cannot escape to impact the whole operating system. Google said that this vulnerability has been exploited in the wild but hasn't provided any specific details as to how. The discovery has been attributed to Shaheen Fazim.

For many organizations, cybersecurity threats are still associated with sophisticated exploits or zero-day vulnerabilities. In reality, a growing number of breaches don't involve hacking in the traditional sense at all. Instead, attackers are logging in using valid credentials obtained elsewhere. **Credential stuffing has become an effective and scalable attack technique in use today**, according to an article from TechRepublic. For IT and cybersecurity decision makers, understanding this threat — and how to defend against it — is critical. And THIS is the reason you hear admonitions to NOT reuse passwords between multiple sites from every corner of the internet userspace.

**Microsoft patched a security flaw with Notepad (?!?!) that left users vulnerable to exploits**, according to an article from Lifehacker. Users could click a malicious link inside a Markdown file in Notepad that would allow attackers to run arbitrary code. Microsoft's push to add AI features to its OS may be contributing to the rise in bugs and security flaws. Users can protect themselves by installing Microsoft's latest security update, which includes the patch for this Notepad glitch. Seriously though … Notepad is a plain, simple (and I mean about as simple as it gets) text

editor. It has NO business being internet-aware, much less connecting to the internet. Someone needs to make Microsoft write “just because you can, doesn’t mean you should” 10,000 times on the blackboard.

*Artist concept from NASA/Aurore Simonnet (Sonoma State University)*

**A surprisingly ravenous black hole from the dawn of the universe is breaking two big rules: It's not only exceeding the "speed limit" of black hole growth but also generating extreme X-ray and radio wave emissions — two features that are not predicted to coexist**, according to an article from LiveScience. The object — a quasar known as ID830 — is an extremely bright and active supermassive black hole (SMBH) that is shooting immense jets of radiation from its poles. It is also emitting intense X-ray emissions, generated by infalling material that swirls around its dark maw at nearly the speed of light. ID830 is exceptionally massive. It already weighed 440 million solar masses around 12 billion years ago, when the universe was approximately 15% of its current age. That makes it over 100 times more massive than Sagittarius A*, the SMBH at the heart of our Milky Way galaxy.

**Researchers have applied a machine learning technique to uncover unexpected features of the non-reciprocal forces that shape the behavior of a many-body system**, according to an article from SciTechDaily. The study, published in *PNAS*, was conducted by experimental and theoretical physicists at Emory University. It combines a specially designed neural network with laboratory measurements from a dusty plasma, a type of ionized gas that contains interacting particles. Unlike most uses of artificial intelligence in science, which focus on analyzing data or making predictions, this work used AI to help reveal previously unknown physical laws. According to the team, the paper delivers the most detailed account so far of the physics governing dusty plasmas, including highly accurate descriptions of non-reciprocal forces.

**That diet soda that you reach for in your refrigerator may not be the best thing to be reaching for, if you’re at all concerned about dementia**, according to a recent study. For those consuming more than one diet soda per day, there was a greater than a four-fold increase in the incidence of dementia. While the full text of the study is locked behind a paywall, you can get the gist of the study results from the abbreviated results listed for free (at the link above). For those consuming sugared soft drinks, there was no statistical increase in the rates of dementia. Hmmmm.

# PCLinuxOS Recipe Corner


## Meatball Bake

Serving size: 4-6

**INGREDIENTS**

2 Tablespoon Olive Oil
5 garlic cloves, minced
1 (6.7-ounce) jar Vegetable Base
¼ teaspoon crushed red pepper flakes
1 yellow bell pepper, cut into strips
1 green bell pepper, cut into strips
1 can (28ozs) Crushed Tomatoes
½ cup dry red wine
¼ cup beef stock
1 teaspoon salt
1 pound pasta shells
1 (12-ounce) bag frozen precooked mini meatballs, thawed
2 cups shredded provolone
Bunch fresh basil, sliced



**DIRECTIONS**

Preheat the oven to 375F.

Heat a large oven-safe pan or skillet over medium-high heat. Add the oil, garlic, vegetable base and pepper flakes. Cook for 1 minute, stirring continuously.

Add the peppers and cook until slightly soft, about 6-8 minutes.

Add the tomatoes, red wine, stock and salt to the pan and then bring to a simmer. Remove from heat and stir the shells into the sauce.

Stir in the meatballs and sprinkle the cheese on top.

Bake for 25-30 minutes uncovered. The meatballs should be cooked through and the pasta tender. Remove from the oven and serve topped with fresh basil.

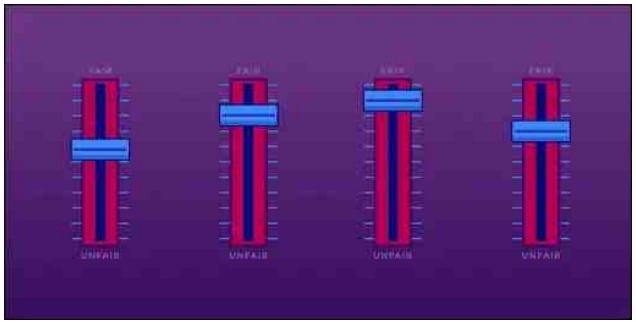
**NUTRITION:**

Calories: 869 Carbs: 100g Sodium: 1528mg
Fiber: 3g Protein: 48.4g



# Search Engines, AI, And The Long Fight Over Fair Use

**by Joe Mullin**
Electronic Frontier Foundation
Reprinted under Creative Commons license



Long before generative AI, copyright holders warned that new technologies for reading and analyzing information would destroy creativity. Internet search engines, they argued, were infringement machines — tools that copied copyrighted works at scale without permission. As they had with earlier information technologies like the photocopier and the VCR, copyright owners sued.

Courts disagreed. They recognized that copying works in order to understand, index, and locate information is a classic fair use — and a necessary condition for a free and open internet.

Today, the same argument is being recycled against AI. It's whether copyright owners should be allowed to control how others analyze, reuse, and build on existing works.

**Fair Use Protects Analysis—Even When It's Automated**

U.S. courts have long recognized that copying for purposes of analysis, indexing, and learning is a classic fair use. That principle didn't originate with artificial intelligence. It doesn't disappear just because the processes are performed by a machine.

Copying works in order to understand them, extract information from them, or make them searchable is transformative and lawful. That's why search engines can index the web, libraries can make digital indexes, and researchers can analyze large collections of text and data without negotiating licenses from millions of rightsholders. These uses don't substitute for the original works; they enable new forms of knowledge and expression.

Training AI models fits squarely within that tradition. An AI system learns by analyzing patterns across many works. The purpose of that copying is not to reproduce or replace the original texts, but to extract statistical relationships that allow the AI system to generate new outputs. That is the hallmark of a transformative use.

Attacking AI training on copyright grounds misunderstands what's at stake. If copyright law is expanded to require permission for analyzing or learning from existing works, the damage won't be limited to generative AI tools. It could threaten long-standing practices in machine learning and text-and-data mining that underpin research in science, medicine, and technology.

Researchers already rely on fair use to analyze massive datasets such as scientific literature. Requiring licenses for these uses would often be impractical or impossible, and it would advantage only the largest companies with the money to negotiate blanket deals. Fair use exists to prevent copyright from becoming a barrier to understanding the world. The law has protected learning before. It should continue to do so now, even when that learning is automated.

**A Road Forward For AI Training And Fair Use**

One court has already shown how these cases should be analyzed. In Bartz v. Anthropic, the court found that using copyrighted works to train an AI model is a highly transformative use. Training is a kind of studying how language works—not about reproducing or supplanting the original books. Any harm to the market for the original works was speculative.

The court in Bartz rejected the idea that an AI model might infringe because, in some abstract sense, its output competes with existing works. While EFF disagrees with other parts of the decision, the court's ruling on AI training and

fair use offers a good approach. Courts should focus on whether training is transformative and non-substitutive, not on fear-based speculation about how a new tool could affect someone's market share.

**AI Can Create Problems, But Expanding Copyright Is the Wrong Fix**

Workers' concerns about automation and displacement are real and should not be ignored. But copyright is the wrong tool to address them. Managing economic transitions and protecting workers during turbulent times are core functions of government. Copyright law doesn't help with those tasks in the slightest. Expanding copyright control over learning and analysis won't stop new forms of worker automation—it never has. But it will distort copyright law and undermine free expression.

Broad licensing mandates may also do harm by entrenching the current biggest incumbent companies. Only the largest tech firms can afford to negotiate massive licensing deals covering millions of works. Smaller developers, research teams, nonprofits, and open-source projects will all get locked out. Copyright expansion won't restrain Big Tech—it will give it a new advantage.


**Fair Use Still Matters**

Learning from prior work is foundational to free expression. Rightsholders cannot be allowed to control it. Courts have rejected that move before, and they should do so again.

Search, indexing, and analysis didn't destroy creativity. Nor did the photocopier, nor the VCR. They expanded speech, access to knowledge, and participation in culture. Artificial intelligence raises hard new questions, but fair use remains the right starting point for thinking about training.

# Screenshot Showcase

*Posted by YouCanToo, on February 6, 2026, running KDE.*

# Wiki Pick: REFInd Boot Manager

*Relevant to all versions of PCLinuxOS*

If your system has modern UEFI firmware, you may wish to install a Boot Manager which can take over (and improve) the work of the Boot Manager built into the firmware.

**Introduction**

rEFInd is a UEFI boot manager which runs when the system first powers up. It scans the EFI System Partition (ESP) looking for bootloaders and displays the results on the screen, allowing the user to choose a bootloader to boot the system.

*Image by Peggy und Marco Lachmann-Anke from Pixabay*

**Installation**

Installing rEFInd is a two-stage process. First the package needs to be installed using Synaptic (search for **refind**). This installs the required packages onto the system but does not configure rEFInd to run automatically at boot. To do that you need to open a root terminal and run:

```
refind-install
```

This will attempt to find your EFI System Partition, copy the rEFInd files to */boot/EFI/EFI/refind* and then create an entry in the firmware Boot Manager for rEFInd and make it the default boot entry so it starts when the system is first powered on. You should peruse the output from the **refind-install** command in case any errors are reported. A successful run should look something like:

```
[root@localhost ~]# refind-install
ShimSource is none
Installing rEFInd on Linux....
ESP was found at /boot/EFI using vfat
Installing driver for ext4 (ext4_x64.efi)
Copied rEFInd binary files
.
Copying sample configuration file as
refind.conf; edit this file to configure
rEFInd.
.
Creating new NVRAM entry
rEFInd is set as the default boot manager.
Creating //boot/refind_linux.conf; edit it
to adjust kernel options.
```

There should now be a new entry in the UEFI firmware boot list which you can check by running (as root):

```
efibootmgr
```

Notice a new **Boot** entry has been created for the rEFInd Boot Manager and that **BootOrder** has been changed to try the rEFInd entry first.

```
BootCurrent: 0003
Timeout: 1 seconds
BootOrder: 0004,0003,0000,0001,0002
Boot0000* Windows Boot Manager
Boot0001* CD/DVD Drive
Boot0002* Hard Drive
Boot0003* pclinuxos
Boot0004* rEFInd Boot Manager
```

### Updating

Although Synaptic will update the rEFInd files in /usr/share/refind it will not update files installed on the EFI System Partition. To update those you will need to re-run the **refind-install** script.

### Configuration

The rEFInd configuration **refind.conf** is located in the same directory as the rEFInd EFI application (usually /boot/EFI/EFI/refind). The default configuration file contains extensive comments explaining all its options, see [https://www.rodsbooks.com/refind/configfile.html Configuring the Boot Manager] for more detailed explanations.

### Passing kernel parameters

In most cases rEFInd will identify the root partition, kernel and kernel parameters automatically. If you wish to adjust the parameters passed to the kernel you can edit the file **refind_linux.conf** which is placed in the same directory as the kernel (usually /boot).

If you do not specify an initrd= parameter, rEFInd will automatically add it by searching for common RAM disk filenames in the same directory as the kernel. If you need multiple initrd= parameters, you must specify them manually in refind_linux.conf.

***Warning!*** *rEFInd only supports detecting one initramfs image per kernel, meaning it will not detect fallback initramfs nor microcode images. They must be specified manually.*

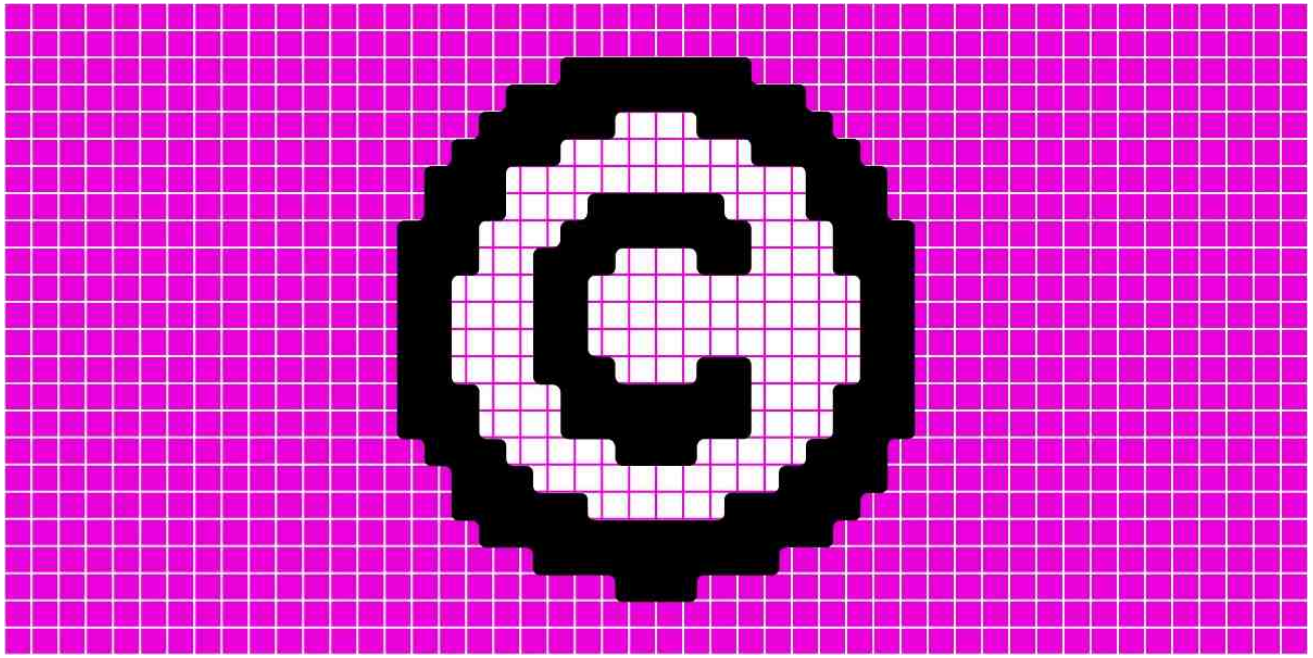
### Manual boot stanzas

If your kernel is not auto-detected, or if you simply want more control over the options for a menu entry, you can manually create boot entries using stanzas in refind.conf. Manual boot stanzas are explained in Creating Manual Boot Stanzas.

Ensure that **scanfor** includes **manual**, or these entries will not appear in rEFInd's menu. Kernel parameters are set with the **options** keyword. rEFInd will append the **initrd=** parameter using the file specified by the initrd keyword in the stanza. If you need additional initrds (e.g. for microcode), you can specify them in **options** (and the one specified by the **initrd** keyword will be added to the end).

*You can view the entire Knowledgebase article here.*

# Rent-Only Copyright Culture Makes Us All Worse Off



**by Corynne McSherry and Rory Mir**
Electronic Frontier Foundation


In the Netflix/Spotify/Amazon era, many of us access copyrighted works purely in digital form – and that means we rarely have the chance to buy them. Instead, we are stuck renting them, subject to all kinds of terms and conditions. And because the content is digital, reselling it, lending it, even preserving it for your own use inevitably requires copying. Unfortunately, when it comes to copying digital media, US copyright law has pretty much lost the plot.

As we approach the 50th anniversary of the 1976 Copyrights, the last major overhaul of US copyright law, we're not the only ones wondering if it's time for the next one. It's a high-risk proposition, given the wealth and influence of entrenched copyright interests who will not hesitate to send carefully selected celebrities to argue for changes that will send more money, into fewer pockets, for longer terms. But it's equally clear that and nowhere is that more evident than the waning influence of Section 109, aka the first sale doctrine.

First sale — the principle that once you buy a copyrighted work you have the right to re-sell it, lend it, hide it under the bed, or set it on fire in protest—is deeply rooted in US copyright law. Indeed, in an era where so many judges are looking to the Framers for guidance on how to interpret current law, it's worth noting that the first sale principles (also characterized as "copyright exhaustion") can be found in the earliest copyright cases and applied across the rights in the so-called "copyright bundle."

Unfortunately, courts have held that first sale, at least as it was codified in the Copyright Act, only applies to *distribution*, not *reproduction*. So even if you want to copy a rented digital textbook to a second device, and you go through the trouble of deleting it from the first device, the doctrine does not protect you.

We're all worse off as a result. Our access to culture, from hit songs to obscure indie films, are mediated by the whims of major corporations. With physical media the first sale principle built bustling second hand markets, community swaps, and libraries — places where culture can be shared and celebrated, while making it more affordable for everyone.

And while these new subscription or rental services have an appealing upfront cost, it comes with a lot more precarity. If you love rewatching a show, you may be chasing it between services or find it is suddenly unavailable on *any* platform. Or, as fans of Mad Men or Buffy the Vampire Slayer know,

you could be stuck with a terrible remaster as the only digital version available.

Last year we saw one improvement with California Assembly Bill 2426 taking effect. In California companies must now at least disclose to potential customers if a "purchase" is a revocable license—i.e. If they can blow it up after you pay. A story driving this change was Ubisoft revoking access to "The Crew" and making customers' copies unplayable a decade after launch.

On the federal level, EFF, Public Knowledge, and 15 other public interest organizations backed Sen. Ron Wyden's message to the FTC to similarly establish clear ground rules for digital ownership and sales of goods. Unfortunately FTC Chairman Andrew Ferguson has thus far turned down this easy win for consumers.

As for the courts, some scholars think they have just gotten it wrong. We agree, but it appears we need Congress to set them straight. The Copyright Act might not need a complete overhaul, but Section 109 certainly does. The current version hurts consumers, artists, and the millions of ordinary people who depend on software and digital works every day for entertainment, education, transportation, and, yes, to grow our food.

We realize this might not be the most urgent problem Congress confronts in 2026—to be honest, we wish it was—but it's a relatively easy one to solve. That solution could release a wave of new innovation, and equally importantly, restore some degree of agency to American consumers by making them owners again.

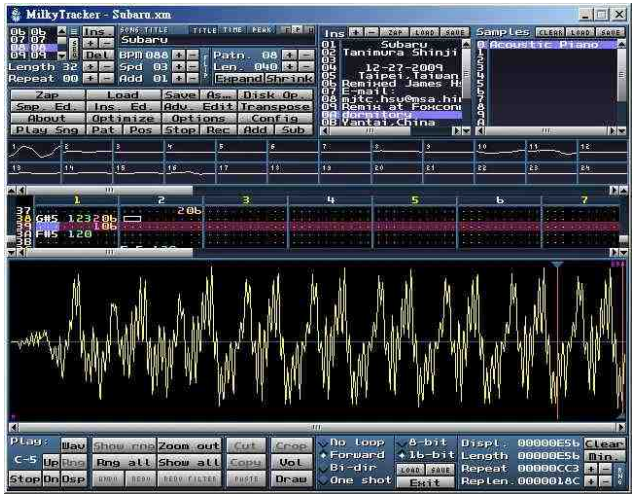


# Screenshot Showcase


***Posted by texstar, on February 8, 2026, running KDE.***

# Making Quality Music Easily & Cheaply On PCLinuxOS, Part 2

**by Alessandro Ebersol (Agent Smith)**




So friends, continuing our series of articles on digital music production in PCLinuxOS, with module trackers, let's delve deeper into some aspects that will be important when we get to the subject of track editing programs, trackers. Why did I decide to continue with the theory? Well, this subject has many concepts that can be somewhat challenging. But I will try to approach these concepts in a way that makes understanding how modular music and trackers are viewed as natural as possible.

So, let's continue discussing these concepts, which will be the cornerstone for our work when we get to the module music editors. And let's also look at resources for working with module music and trackers, such as places to download samples and auxiliary programs.

**Diving into module tracker music theory**

There are several elements common to any tracker program: samples, notes, effects, tracks (or channels), patterns, and orders. Let's take a look at what each of these elements is.

- A sample is a small digital sound file of an instrument, voice, or other sound effect. Most trackers allow part of the sample to be repeated simultaneously with a note.

- A note designates the frequency at which the sample is played. Increasing or decreasing the playback speed of the digital sample raises or lowers the pitch, simultaneously with the notes. English notation is used here: C, C# for Do, Do#, Re.

- An effect is a special function applied to a specific note. These effects are then applied during playback via hardware or software. The main tracker effects include volume, portamento, vibrato, retrigger, and arpeggio.

- A track (or channel) is a space where a sample is played back. While the original Amiga trackers only provide four tracks due to hardware limitations, modern trackers can mix an unlimited number of virtual channels through software mixing. Tracks have fixed tempos, although the tempo and pitch can be increased or decreased depending on the composer's preference. A basic drum set could therefore be arranged by placing the ‘bass’ rhythm on lines 0, 4, 8, 12... of one track, some hithats on lines 2, 6, 10, 14, etc. of a second track. Of course, the ‘bass’ and ‘hithats’ can be placed on the same track if the samples are short enough. Otherwise, the previous sample will be interrupted when the next one starts.

- A pattern is a group of tracks played simultaneously that represents an entire section of a song. A pattern is intended to represent an equal number of bars in a musical composition.

- An order is the part of a sequence of patterns that defines the meaning of the piece. Patterns can be repeated in any order to save time and space in the file.

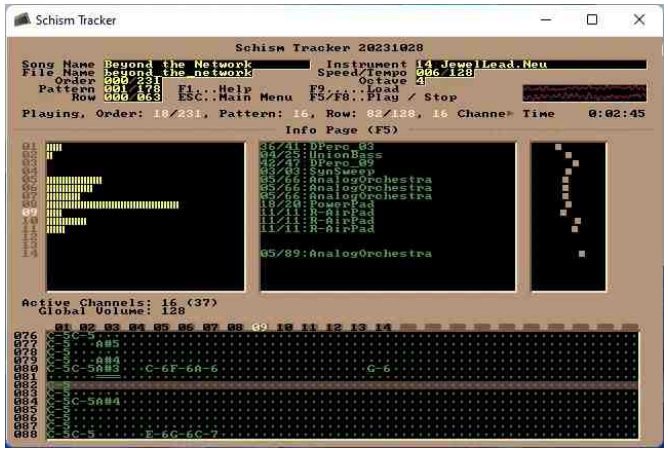
**How it works: The module music tracker technique**

The image on the next page is a screenshot of a tracker, a module music editor, and we can see the elements that make up this interface:

- An instrument/sample window

• A channels window

• A window of the song




Sound production is based on samples, which can be simple small recordings made with a microphone or line input. The sound quality will depend on the sample rate at which it was recorded. This sampling frequency is usually between 8 kHz (telephone sound quality) and 48 kHz (movie sound quality). If a sound is represented as a wave on a coordinate axis, the y-axis represents the intensity and the x-axis represents the frequency of the sound.

Sound can be altered in the following ways:

**Volume:** It will increase by stretching the y-axis and decrease by compressing the same axis.

**Pitch:** Stretching the wave along the x-axis produces a lower sound, while compressing the wave makes the resulting sound higher. In this way, starting from a sound that corresponds to a musical tone, all other tones in the scale can be obtained.

Two other common effects are looping and panning.

**Looping** is when a sound, when it reaches the end, continues from the beginning. This way, you can create a continuous tone over time or a rhythmic sound.

**Panning** is the independent volume change of the left and right channels. It is used to move a sound from one side to the other in stereo. The Commodore Amiga sound chip had 4 channels, so it could play four tracks by adjusting the pitch and volume independently of each other. Therefore, the tracker software did not need to mix the tracks, but send them directly to the sound chip. The panning effect, which mixes sound across two channels by moving it from one to the other, did not yet exist. Channels 1 and 4 formed the left channel, and channels 2 and 3 formed the right channel. With the arrival of the Gravis Ultrasound sound card, it became possible to mix up to 32 channels independently of each other, allowing for panning. Other sound hardware (from Sound Blaster to PC Speaker), which offered no more than 2 channels (right and left if stereo), meant that the different channels were mixed by software, consuming much more processor resources, but with the improvement in their power, the composition of several high-quality tracks became possible on personal computers: normal PCs. An important advantage of software mixing is the precise and perfectly synchronized handling of samples.

In the Amiga era, due to the scarcity of channels, more than one instrument could be played on a channel, meaning you could have more samples being played on one of the channels, not simultaneously, but sequentially. Obviously, the sample for each instrument had to be specified. But how does this happen? Let's analyze how the magic of music occurs in modules.

**Inside the trackers interface**

We can get a little discouraged when someone talks about “programming” a track, as it sounds a bit complicated. In fact, you are closer to coding a track here than by other means, but there are some advantages to this method of music composition and several resources available to help you learn it. Let's see what's inside:


The main screen we have is the Music Screen (1), where all the tracks reside and you will see the data flying gloriously during playback. The Instrument Panel (2) houses all the samples and instruments within your song—these are your sound sources, so you can think of it as a kind of “project pool” in modern terms.

Trackers use Patterns (3) to form sections of a song, rather than specifying line by line—these patterns form groups of tracks together, simplifying the arrangement of chorus, breakdown, and intro sections. Some trackers, such as LSDJ and NerdSeq, have the ability to chain patterns together to form larger sequences of patterns, if you want, for example, a longer chord progression.

Nowadays, we mainly use the mouse to do most of the navigation within a DAW, but trackers started when the keyboard was king! Therefore, they are known for their extensive use of keyboard shortcuts for quick and repeated actions. Find the shortcuts you need for your tracker and you won't regret it!

**Main components**

Trackers share a basic set of features with their counterparts in any other DAW (Digital Audio Workstation):

- A sample or instrument
- A track to play them on
- Effects for that track
- Music data

All instruments and samples are sequenced in a track and displayed in lines composed of notes, instruments, and effects together. As the music plays, each line is triggered from top to bottom.

A track line might look like this:

0027 C4 12 0A 04

- 0027 represents the line or time step at which the note will be played
- C4 is the note and octave at which it will be played
- 12 is the sample or instrument number

The last two digits are connected:

- 0A is the effect parameter (e.g., panning, volume, vibrato)
- 04 is the value or amount of the effect

You can change any of these values as you wish, to control the individual volume of the notes, the panning, the offset, or even change the instrument from one note to another! In a later line, we could write:

031 F#4 11 0A F0

So, four steps later, he would play an F# in octave 4, changing the instrument/sample to something else and altering the effect parameter to a higher number, perhaps to pan to the right.

The song data will define the tempo of the track, as well as the number of lines we have per beat for alternate tempos and various other settings, depending on the tracker.

**The Effect column**

This column tells the tracker which effects (if any) to apply and to what degree—a simple example would be changing the volume or panning position. Next to each note, you can place a parameter and a value in the corresponding row to change them. The effects vary depending on the file format you choose (MOD has some effects, but other formats, such as XM or S3M, have effects that the MOD format does not have, so when choosing the format, be aware of which effects you will be able to use).

To illustrate, below are some from the Renoise tracker, which are useful because they use the full character set:

**0A - Arpeggio**

**0G - Glide**

**0V - Vibrato**

**0T - Tremolo**

**0R – Retrigger**

As I wrote above, effects are defined differently between trackers and between file formats, and are most commonly referenced in hexadecimal numbers (see below). They can include note slides, offsets, pattern breaks, sample start point, vibrato, arpeggio, and many other parameters. In some cases, the effect value is split, for example, with tremolo—the first digit being the rate and the second being the depth.

0T 28 - A slow, deep tremolo

0T F2 - A fast, light tremolo

Many modern trackers also have master track effects to process the entire mix, most relevant for use with VSTs (Virtual Studio Technology, virtual effects and instrument technology).

**Hexadecimals, get used to them**

Trackers tend to use hexadecimal numbers to count. The advantage of this is that we can count up to a high number (255) using only two characters - the disadvantage is that, initially, this can confuse your mind! It's not such a complicated concept: in the decimal system, we count in groups of ten (10, 20, 30, 40, 50...), while in hexadecimal we count in groups of sixteen using the additional characters A, B, C, D, E, F:

**0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F**

and then

**10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 1A, 1B, 1C, 1D, 1E, 1F**

Then

**20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 2A, 2B, 2C, 2D, 2E, 2F**

And so on until we reach FF, which is 255 in decimal. The Dirtywave M8, a hardware tracker, has a useful hexadecimal table to help with conversion—you'll find that it becomes second nature. In fact, this manual is very comprehensive and provides excellent information on the theory of music trackers, so I recommend downloading this file as study material.

If you want to automate something like a sample loop point from 0 to 255, it's useful to know some important hexadecimal points:

0% = 00

25% = 40

50% = 80

75% = C0

100% =FF

**Some interesting resources**

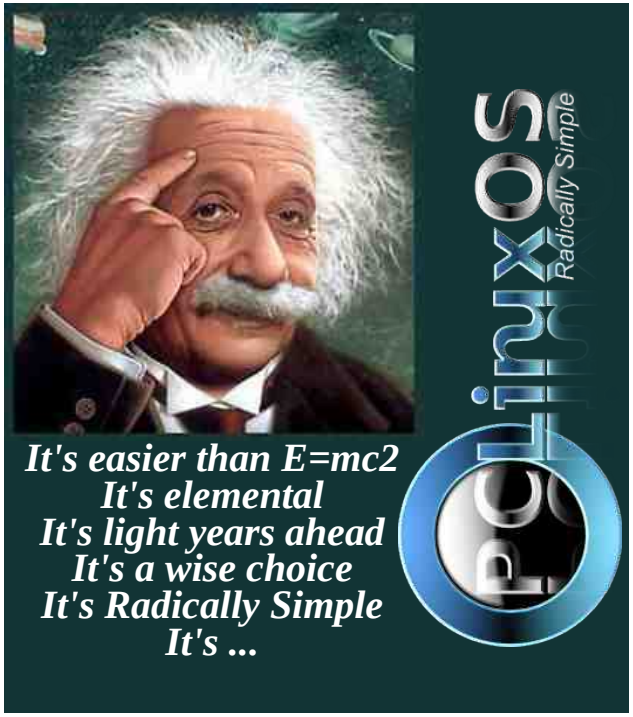
Getting started with LSDJ

Protracker tutorials

Modarchive A collection of music modules

Collection of Samples:
https://www.woolyss.com/tracking-samples.php

Well, I hope you enjoyed a little more theory and concepts. It may seem boring at first, but it's better to have a solid foundation before starting to work with the programs in our next article. Greetings, and see you then!



# GIMP Tutorial: Layer Masks, Part 1

**by Meemaw**

I've been asked several times to do an article on Layer Masks. A layer mask is actually fairly easy to do but sometimes hard to understand, since most of the time when you're working with an image, you want the whole thing to show. However, in some instances, you can change the effect by using a layer mask.

I referred to a couple of places to get help with this subject. One was one of Davies Media Design's tutorials, and the other was one from The GIMP Tutorials.

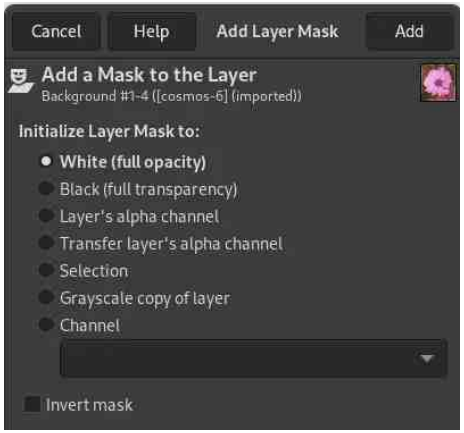
A layer mask in GIMP allows you to control the transparency of different parts of a layer, enabling you to hide or reveal portions of the layer beneath it.

The most common choices are **White (Full opacity)** and **Black (Full transparency)**, but you'll have to decide which is best for your particular situation.

**White (Full opacity)** will keep the layer fully visible until you start painting with black pixels onto the layer mask, hiding the parts of the image that you don't want to keep. I used this several years ago, on one of my first GIMP tutorials. In that one, I used two copies of the same photo, with one of them desaturated and placed on top of the colored layer. I painted on the desaturated layer and brought out the lower colored layer. It created a cool effect.

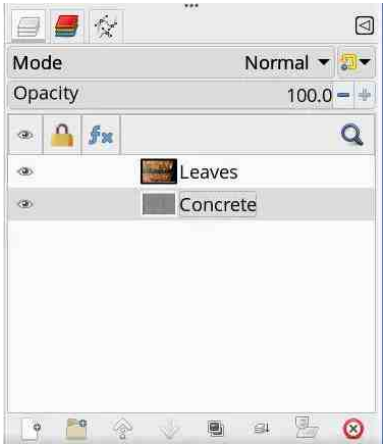
**Black (Full transparency)**, the layer will immediately be completely masked out and hidden, which makes it much harder to work with because you can't see the layer contents while painting your mask. We used this a couple of months ago, on the picture we "blew up". I had two copies of the same photo again, but I used the layer mask to bring out the pieces of the top layer that I wanted to show (top, right).

When you decide what effect you want, you can right-click the layer you want to affect, and choose **Add Layer Mask**. You'll get the following window, where you can choose the type of layer mask you want. The default choice is white, but if you don't reset things when you exit, another type may be chosen.

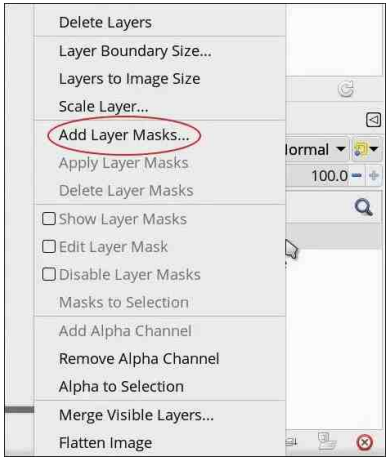


Maybe you want to design a path through fallen leaves. I found an image of fallen leaves I really like, so we'll use that.

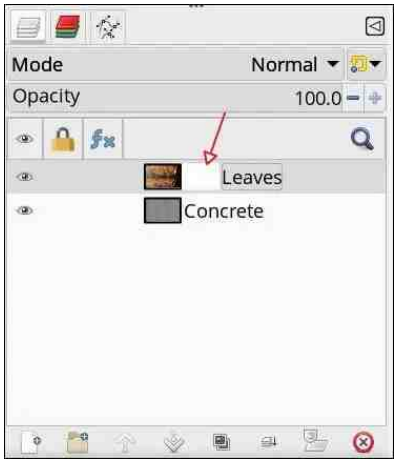
This path is going to be a sidewalk, so I found a graphic of concrete, and loaded it into GIMP, making it the lower layer.




Now you want to change the leaf image, so the concrete shows through like a path or sidewalk. Choosing the leaf image layer, right-click on the layer and choose **Add Layer Masks**. The choice in the popup window will be White (Full Opacity).



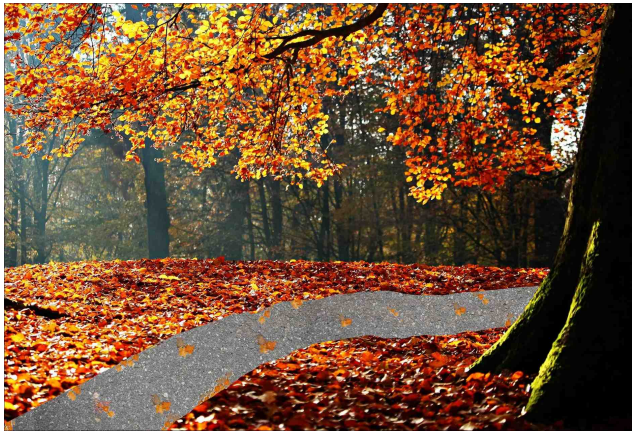

Now you see it in place.




To use the mask, click on the mask, change your brush color to black, and stroke where you want the leaves to disappear. Adjust the brush size to something that works for you. Depending on the image size, the brush could be any size. This image is 1920 x 1260 px, so I made the brush 50px (top, right).

As you draw, you will see the black marks on the layer mask. If you make a mistake, change your color to white, and paint over the mistake, and you'll get the leaves back. Remember to change your color back to black to finish the path.

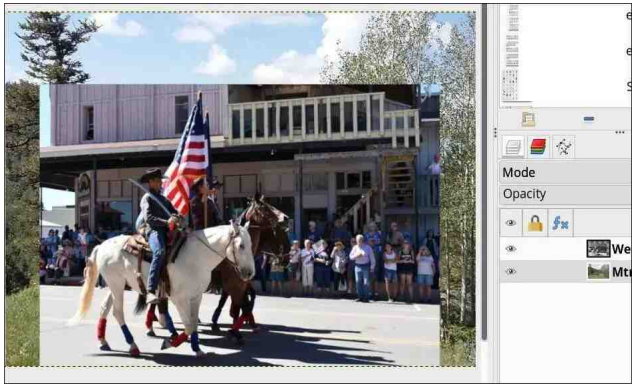
The next thing I did was add some leaves back onto the path (they don't stay clean for long). However, since the layer mask erased the leaves, I had to add back to the concrete layer, or they wouldn't have been visible. You could also add a transparent layer on top and place them there.



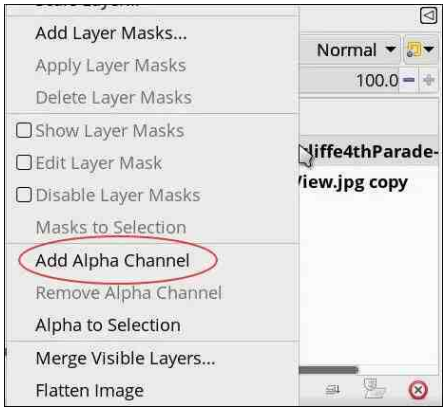
I would do a bit more to this, like adding shadows, but that's the basics of a layer mask.

The next mask on the list is the **Black (Full Transparency)**, and it works when you want your layer mostly invisible and only want to bring out parts of it. Suppose you want to feature a certain group, but in a different background. I had this group I saw in a 4th of July parade a few years ago, but wanted to put them in a mountain scene.

I opened these images in GIMP using **Open as Layers**. They opened in the same project. I had to resize the horse layer to put the group into the mountains.




The first thing we will do is add an alpha channel to the top layer (horses). Right-click the layer and choose **Add Alpha Channel**. It has to have an alpha channel for the "paint" to be transparent.




Now, right-click the top layer again and choose **Add Layer Masks**. This time we'll choose **Black (Full Transparency)**. (top, right)

When you click OK, your layer will disappear. Since I scaled that layer down, I can see the edges of the layer in the other image. Since I already started to paint with white, I can also see part of the horse. To make it easier to paint


accurately, I will alternate between the mask and choosing **Disable Layer Mask** in the layer menu so I can paint what I need to show. Uncovering the horse group seemed easier to me than covering the rest of the photo.

You can see that I've got a lot of the horses filled in, but I haven't done the shadows yet. For that, I'm going to choose a grey to paint with because it will leave a bit of opacity, and

hopefully some of the grass will show through. The color turned out to be a light grey (cecbc6). If it's not dark enough while letting in some of the background, lighten your grey.

I have to "fine tune" it, but I have the basics done.

Of course, in GIMP, you can also use your scissors tool, cut out the horse group and insert it into the mountain image. There's always more than one way to do something. We'll visit the other types of layer masks soon.







## Screenshot Showcase


*Posted by Ramchu, on February 7, 2026, running KDE.*

# Setting Up a DIY NAS with OpenMediaVault, Part 2

**by David Pardue (kalwisti)**

**Access Your Shared Storage Folder in PCLinuxOS**

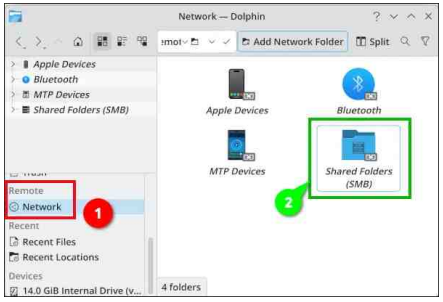
After you have designated/added the storage disk from your NAS PC, created a shared folder for NAS storage, enabled the SMB/CIFS service and configured user access, you will need to test your setup to verify whether you can access your shared NAS folder.

The subsections below illustrate how to access the shared NAS folder in KDE Plasma (Dolphin file manager), Xfce (Thunar file manager), MATE (Caja file manager), Openbox and/or LXDE (PCManFM file manager).

**KDE Plasma 6.5.5 (Dolphin File Manager)**

On the left side panel, look for **Remote** > **Network**.

Click on the **Shared Folders (SMB)** folder to open it.



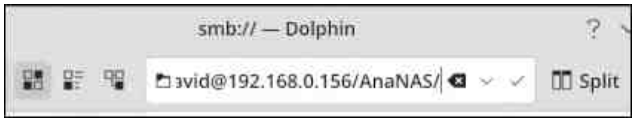

In the Location bar, type:

**smb://yourusername@NAS.IP.address/Name_of_Your_Shared_NAS_Folder/**

In my case, this is:

**smb://david@192.168.0.156/AnaNAS/**

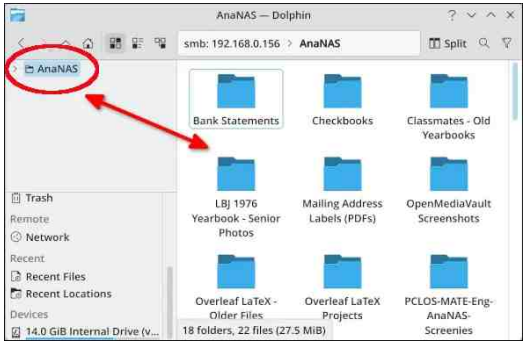
(I named our shared NAS folder "AnaNAS." "Ananas" is the word for ‘pineapple’ in a variety of languages; I thought it would be a fruity tip of the hat to my original plan of using a Raspberry Pi for this project.)



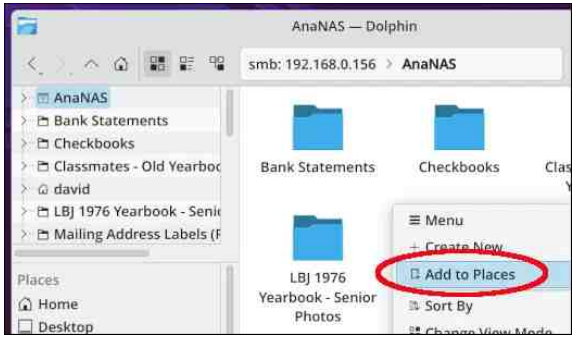

An Authentication dialog opens.

Type in your NAS user password (the one that you chose in OMV's workbench).

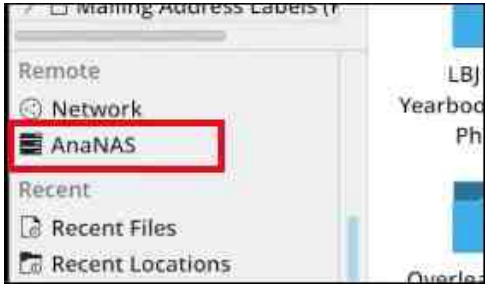
Click on the **OK** button. The shared NAS folder should open.


Right-click in an empty space of the shared folder display. Choose **"Add to Places."**




An entry for the shared NAS folder should appear in **Places** > under the **Network** category.



After configuring this, the next time that you log in to KDE Plasma and click on the shared NAS folder entry, you will see an Authentication dialog open.

Type in your OMV NAS user credentials and click the **OK** button. Your shared NAS folder should open.

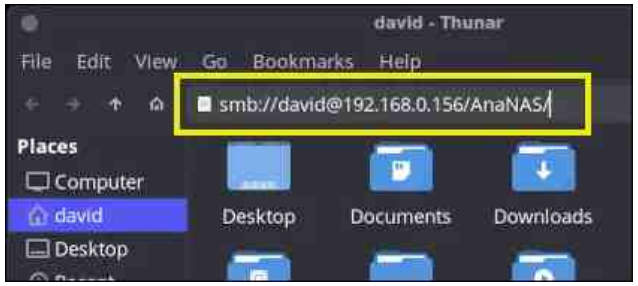

**Xfce (Thunar File Manager)**

Open Thunar. In the Location bar, type:

**smb://yourusername@NAS.IP.address/Name_of_Your_Shared_NAS_Folder/**

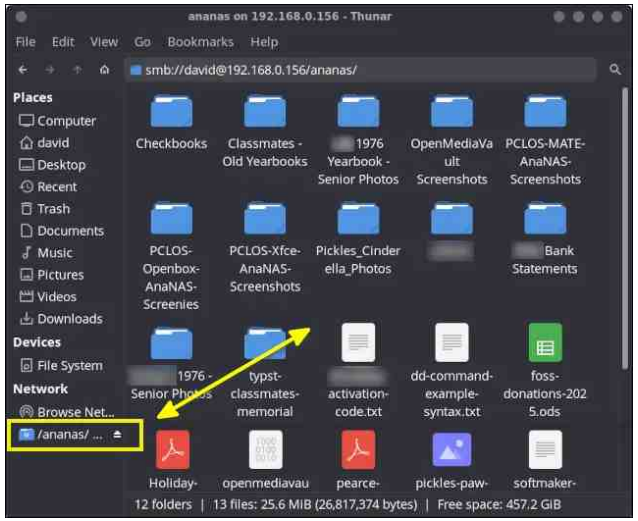
In my case, this is:

**smb://david@192.168.0.156/AnaNAS/**

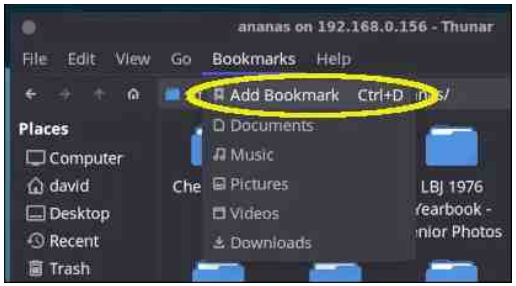



An Authentication dialog will open. Enter your OMV user password and click on the **Connect** button.


The shared NAS folder should open in Thunar.




Afterwards, you can add a bookmark for your shared storage folder by clicking on the **Bookmarks** menu > and choosing **Add Bookmark** (right, top).




**MATE (Caja File Manager)**

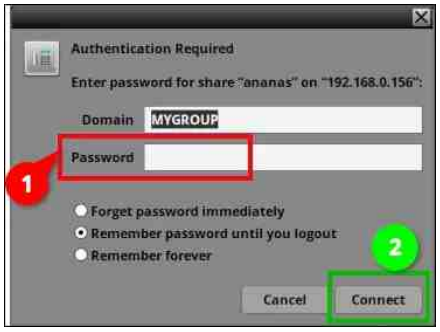
Open Caja. In the Location bar, type:

**smb://yourusername@NAS.IP.address/Name_of_Your_Shared_NAS_Folder/**

In my case, this is:

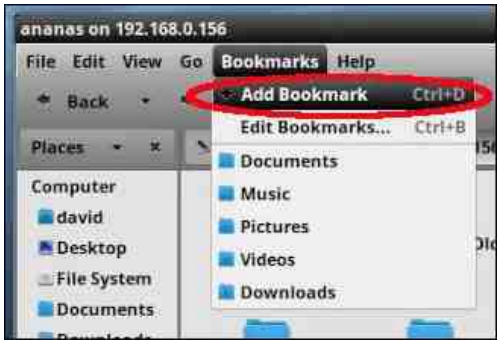
**smb://david@192.168.0.156/ananas/**


An Authentication dialog will open. Enter your OMV user password and click on the **Connect** button.



The shared NAS folder should open in Caja.


Afterwards, you can add a bookmark for your shared storage folder by clicking on the **Bookmarks** menu > and choosing **Add Bookmark**.




**Openbox and LXDE (PCManFM File Manager)**

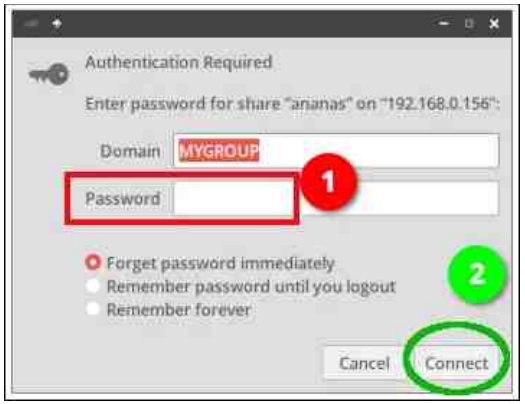
Open PCManFM. In the Location bar, type:

**smb://yourusername@NAS.IP.address/Name_of_Your_Shared_NAS_Folder/**

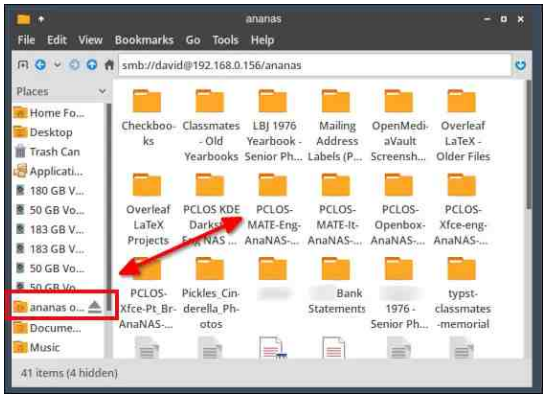
In my case, this is:

**smb://david@192.168.0.156/ananas/**

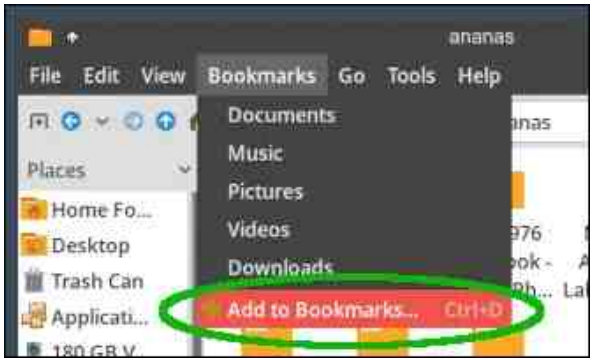

An Authentication dialog will open. Enter your OMV user password and click on the **Connect** button.

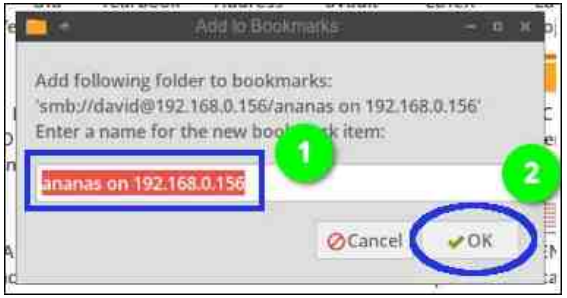



The shared NAS folder should open in PCManFM.




Afterwards, you can add a bookmark for your shared storage folder by clicking on the **Bookmarks** menu > and choosing **Add to Bookmarks**.




**Conclusion**

I hope that my article has somewhat demystified the process of setting up a DIY NAS. Our network knowledge is basic, but my son and I were able to create/configure a NAS — thanks to OMV and some excellent online guides. We enjoyed tackling this project together; we gained an appreciation for hardware and software that simplifies the arcana of networking protocols.

The total cost of the components was around $225, which was almost the same price as a

CanaKit Raspberry Pi 5 Starter Kit (8 GB) plus the PNY 500 GB SSD that I purchased. Although I admire the ingenuity of the Raspberry Pi community and would like to experiment with one, I am happy with our DIY NAS solution. It has been performing well for our home office file sharing via SMB/CIFS and FTP.

**Additional Resources**

Barnatt, Christopher. Explaining Computers. "Mini PC OpenMediaVault NAS." YouTube, 5 Nov. 2023. (19 min., 47 sec.)

(Although this video is from 2023 and uses a superseded version of OMV [6.5.0], I recommend it because Prof. Barnatt provides clear, concise explanations.)

OMV Forum (with a friendly community): https://forum.openmediavault.org/

Pande, Ayush. "Building a NAS with OpenMediaVault Is Easy — Here's How It's Done." XDA Developers, 7 Nov. 2024.





# Screenshot Showcase


*Posted by present_arms, on February 4, 2026, running openbox.*

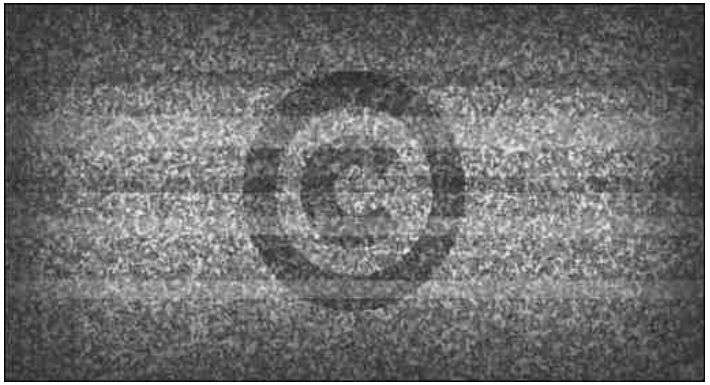
# Copyright Kills Competition

**by Tori Noble**
Electronic Frontier Foundation
Reprinted under Creative Commons license

Copyright owners increasingly claim more draconian copyright law and policy will fight back against big tech companies. In reality, copyright gives the most powerful companies even more control over creators and competitors. Today's copyright policy concentrates power among a handful of corporate gatekeepers—at everyone else's expense. We need a system that supports grassroots innovation and emerging creators by lowering barriers to entry—ultimately offering all of us a wider variety of choices.

Pro-monopoly regulation through copyright won't provide any meaningful economic support for vulnerable artists and creators. 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 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's no reason to think that these same companies would treat their artists more fairly now.

**AI Training**

In the AI era, copyright may seem like a good way to prevent big tech from profiting from AI at individual creators' expense — it's not. In fact, the opposite is true. Developing a large language model requires developers to train the model on millions of works. Requiring developers to license enough AI training data to build a large language model would limit competition to all but the largest corporations—those that either have their own trove of training data or can afford to strike a deal with one that does. This would result in all the usual harms of limited competition, like higher costs, worse service, and heightened security risks. New, beneficial AI tools that allow people to express themselves or access information.

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, the first of many copyright lawsuits over the use of works train AI. ROSS Intelligence was a legal research startup that built an AI-based tool to compete with ubiquitous legal research platforms like Lexis and Thomson Reuters' Westlaw. ROSS trained its tool using "West headnotes" that Thomson Reuters adds to the legal decisions it publishes, paraphrasing the individual legal conclusions (what lawyers call "holdings") that the headnotes identified. The tool didn't output any of the headnotes, but Thomson Reuters sued ROSS anyways. A federal appeals court is still considering the key copyright issues in the case — which EFF weighed in on last year. EFF hopes that the appeals court will reject this overbroad interpretation of copyright law. But in the meantime, the case has already forced the startup out of business, eliminating a would-be competitor that might have helped increase access to the law.

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. The cost of licensing enough works to train an LLM would be prohibitively expensive for most would-be competitors.

**The DMCA's "Anti-Circumvention" Provision**

The Digital Millennium Copyright Act's "anti-circumvention" provision is another case in point. Congress ostensibly passed the DMCA to discourage would-be infringers from defeating Digital Rights Management (DRM) and other access controls and copy restrictions on creative works.

In practice, it's done little to deter infringement —after all, large-scale infringement already invites massive legal penalties. Instead, Section 1201 has been used to block competition and innovation in everything from printer cartridges to garage door openers, videogame console accessories, and computer maintenance services. It's been used to threaten hobbyists who wanted to make their devices and games work better. And the problem only gets worse as software shows up in more and more places, from phones to cars to refrigerators to farm equipment. If that software is locked up behind DRM, interoperating with it so you can offer add-on services may require circumvention. As a result, manufacturers get complete control over their products, long after they are purchased, and can even shut down secondary markets (as Lexmark did for printer ink, and Microsoft tried to do for Xbox memory cards.)

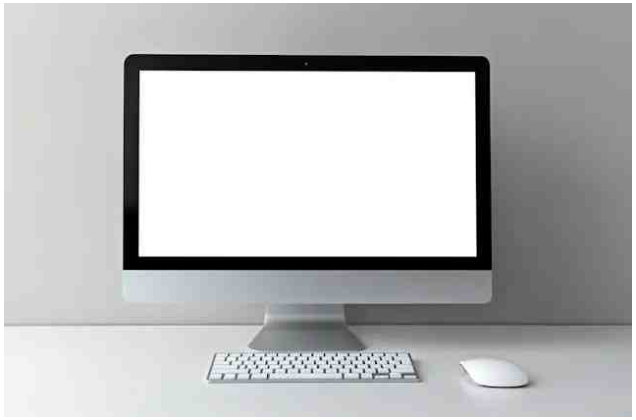
Giving rights holders a veto on new competition and innovation hurts consumers. Instead, we need balanced copyright policy that rewards consumers without impeding competition.

# Screenshot Showcase

***Posted by piratejumbo, on February 4, 2026, running KDE.***

# Digital Hygiene 101: A Doctor's Prescription For Your Online Health

**by Hamza Mousa**
Founder of Medevel
Reprinted with permission



I still remember the first time I fully understood the importance of a sterile field. In medical school, "scrubbing in" wasn't just about washing your hands; it was a ritual. You follow a strict process, fingertips to elbows, specific timing, no touching anything unsterilized afterwards, because skipping even a small step could introduce an infection that brings down the whole system (the patient).

Ironically, my life in tech follows the exact same principle. I've been a Linux enthusiast since I installed Slackware in the late 1990s, and if there is one thing that connects medicine and software engineering, it is this: **Prevention is always cheaper than the cure.**

Just as we practice personal hygiene to prevent disease, we must practice **Digital Hygiene** to prevent data breaches, identity theft, and the slow "rot" of our digital lives. Whether I'm diagnosing a patient or debugging a Next.js application, the mindset is the same.

Here is my prescription for keeping your digital life healthy.

**What Is Digital Hygiene?**

**Digital Hygiene** (or Cyber Hygiene) refers to the routine habits and practices you perform to keep your devices, data, and online identity secure and organized. It isn't a one-time "fix", you don't brush your teeth once a year and expect no cavities. Similarly, you cannot install an antivirus once and assume you are safe forever. It is a continuous maintenance routine designed to preserve your **digital sovereignty**.

**The Checklist: 5 Steps To Digital Sovereignty**

**1. Password Management (The First Line Of Defense)**

Stop reusing passwords. If you use the same password for your banking and that random forum you signed up for in 2015, you are one data breach away from a disaster.

**The Fix:** Use a **Password Manager** (like Bitwarden, which you can even self-host).

**The Habit:** Enable **Two-Factor Authentication (2FA)** everywhere. It's the digital equivalent of a double-lock on your door.

The following list contains the best open-source password managers that we collected, tested, and used over the years.

**42 Open-source Free Password Managers for Windows, Linux, macOS, iOS, and Android**

**13 Open-source, free Password managers for macOS**

**Top 13 Free Self-Hosted Password Managers for Teams and Agencies in 2025: Secure Your Data Today!**

**2. Software Updates (Your Digital Vaccination)**

I know getting that "Update Available" notification is annoying, especially when you are in the middle of a workflow or deep in a coding session. But in the security world, we call those updates "**patches**" for a reason, they cover up the holes that hackers use to get in.

Think of an outdated system like a house with the windows smashed out during a zombie apocalypse. When you ignore an update, you

aren't just being lazy; you are effectively **inviting the zombies and vampires inside**. You are rolling out the red carpet for malware to suck the life out of your data.

**The Fix:** Treat updates like vaccinations. They provide herd immunity for your network.

**For macOS Users:** Don't fall for the myth that "Macs don't get viruses." That hasn't been true for a decade. Apple pushes critical security responses for a reason. If you ignore them, you are leaving the castle gates wide open.

**For Linux Users:** I know we love our uptime, and rebooting feels like defeat. But running sudo apt update && sudo apt upgrade ([alternative: 'su -c 'apt update && apt upgrade'], or pacman -Syu if you're brave) isn't just maintenance, it's hygiene. A kernel vulnerability doesn't care how cool your tiling window manager is.

**Don't Forget the Apps:** It's not just the OS. An outdated browser extension, an old version of Zoom, or that PDF reader you installed three years ago? Those are the "**trojan horses**". Hackers love them because nobody checks them.

**Rule of Thumb:** If it connects to the internet, it needs to be updated. Period.

### 3. Digital Decluttering (Removing "Zombie Apps")

Over time, our devices accumulate "digital plaque." Unused apps on your phone or old accounts you haven't logged into for years are liabilities. They track your data and provide attack vectors.

**The Fix:** Once a month, review your apps. If you haven't used it in 6 months, delete it. Close old accounts to reduce your **digital footprint**.

On macOS, it is important, as it takes SPACE.

### 4. Data Backups (The 3-2-1 Rule)

As a developer & a doctor, I've stared at the black screen of death, and I can tell you that hard drives fail, SSDs degrade, and ransomware strikes without warning. I have seen years of family photos and critical source code vanish into the void simply because someone trusted a single drive. In the world of hardware, it is rarely a matter of if disaster strikes, but when.

**The Fix:** You need a continuity plan: the **3-2-1 Rule**. Keep **3** copies of your critical data. Store them on **2** different media types (for example, your local machine and an external SSD).

Finally, ensure **1** copy is offsite, like an encrypted cloud service. If a fire or theft wipes out your physical office, that offsite backup is the heartbeat that keeps your digital life alive.

**BackupPC is a system backup tool that enables you to back up your operating system to a remote server disk.**

**Securely Backup your Data and Files to the Cloud with Duplicati**

**Areca Backup is a Free Backup and Recovery Solution for Windows and Linux Systems**

### Special Round: Essential Security Tips for Windows Users

Look, everyone knows I'm a Linux guy. To me, Linux isn't just an OS; it's a mindset. But I know many of you rely on **Windows** for work or gaming. Windows is the biggest target for malware simply because it has the most users. If you are on Windows, you need to be extra vigilant.

**Here is how to lock it down:**

**Debloat the System:** Windows comes pre-installed with "bloatware" (ads, trial games, unnecessary tracking). Use tools or scripts to remove these. Less software installed means fewer security holes.

**Enable BitLocker:** If your laptop gets stolen and your drive isn't encrypted, your password won't stop a thief from reading your data. Turn on BitLocker (device encryption) immediately.

**Respect Windows Defender:** You rarely need expensive third-party antivirus software anymore. Windows Defender is actually quite capable now, but only if you keep it updated and don't turn it off.

**Create a Standard User Account:** Don't use your PC as an "Administrator" for daily tasks. Create a standard account for daily use. If

malware tries to install itself, it will fail because it won't have the permissions to write to system files.

**24 Windows Cleaner Apps and Scripts to Keep Your Windows Clean and Fast in 2025!**

**29 Free Windows Cleaner Apps to Keep Your System Clean, Fast and Optimized**

**Conclusion: Make It A Lifestyle**

Whether it's creating a sterile environment for a patient or a secure environment for your data, the goal is safety and longevity. Start small. Pick one of these habits today, maybe just changing that one weak password you've been using for everything, and build from there.

Stay safe, stay private, and keep your systems clean.

***About The Site & Author***

*Medevel.com is a restart of an old project, Goomedic.com, when we used to blog about medical/ healthcare related open-source projects. The writers are also medical doctors doing software development, as well as open-source enthusiasts and Advanced Linux users.*

*Medevel.com is writing articles about open source with a primary focus on medical, science projects.*

*Medevel.com is on a mission to promote open source to healthcare sector users like doctors, nurses, healthcare IT specialists, open-source community, researchers.*

*Medevel.com's team is writing about visualization, medical imaging, lab-ware, medical records (EMR, EHR),* ***clinical practice management software, digital pathology, medical simulation, & data analytics apps.***

***Medevel.com is focusing on:***

*Open source technologies for Healthcare*

*Privacy-focused applications*

*Medical Imaging: DICOM/PACS solutions*

*Electronic Medical Records/Electronic Health Records*

*Medical Visualization & Simulation*

*HIPAA & GDPR compliant solutions*

*Self-hosted Open-source solutions*

*Linux Applications*

*Medical Mobile apps for Doctors & patients (Android, & iOS)*

*We are also writing reviews about some open-source software, & projects which we find useful for our audience, aiming to help open-source software developers to reach more audiences.*

***Authors***

***Hamza Mousa:*** *A physician with programming skills, Linux user since late 1990s, Open-source supporter. He is also a former PCLinuxOS user.*

***Desoky Mo:*** *A physician interested in Open Source, programming, machine learning, AI and technology in general.*

***M.Hanny Sabbath:*** *Computer science and engineering graduate, with an ongoing M.Sc in computer science. Founder of FOSSPost.org. An open-source software developer and technical writer for more than 10 years.*

# Tip Top Tips:
# Have You Backed Up Your Install?

***Editor's Note:*** *Tip Top Tips is a semi-monthly column in The PCLinuxOS Magazine. Periodically, we will feature – and possibly even expand upon – one tip from the PCLinuxOS forum. The magazine will not accept independent tip submissions specifically intended for inclusion in the Tip Top Tips column. Rather, if you have a tip, share it in the PCLinuxOS forum's "Tips & Tricks" section. Occasionally, we may run a "tip" posted elsewhere in the PCLinuxOS forum. Either way, share your tip in the forum, and it just may be selected for publication in The PCLinuxOS Magazine.*

This month's tip is from **ramchu**.

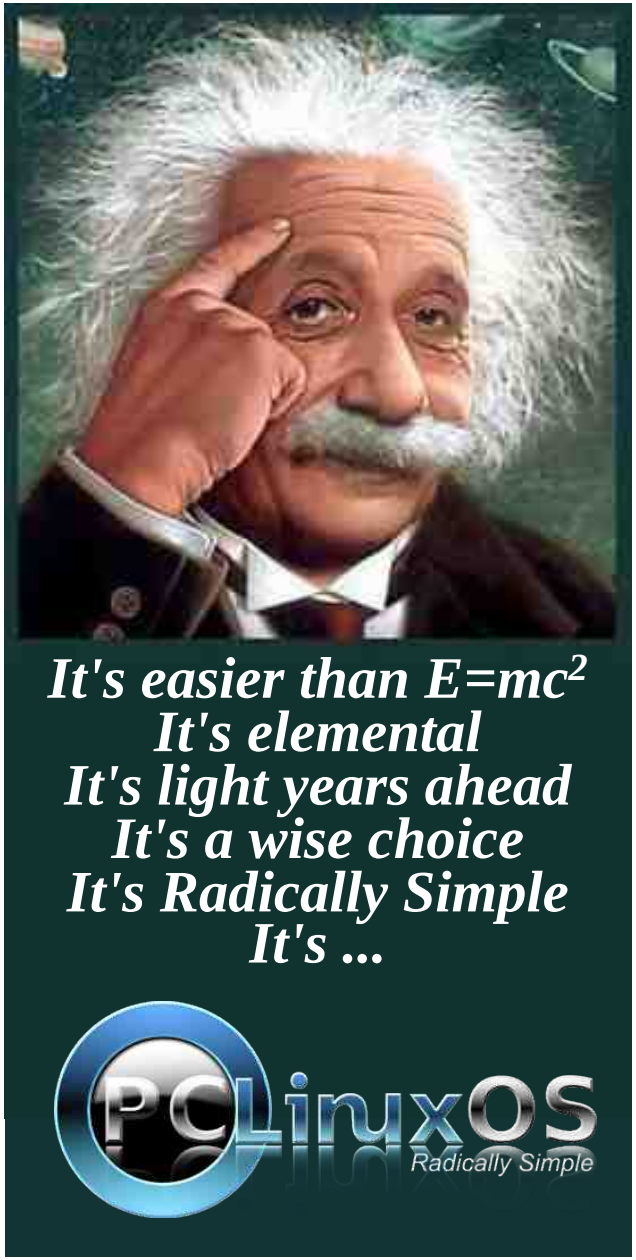
I more than likely over do it, but I use Timeshift, Grsync, and MyLiveGTK (original version) Timeshift runs daily and monthly backups, I keep five daily backups and one monthly backup. This backs up the operating system.

Once a week I run Grsync and backup my home/user partition onto a USB attached hard drive.

Also once a week I use MyLiveGTK and create a remaster of the complete system, excluding the extremely large files and folders, and this gets put on a USB stick running Ventoy.

This way I have options, and if I need, I can be back up and running in a very short time if I have a bad update, drive failure, or get to dinking around and crash the system.





# PCLinuxOS Recipe Corner Bonus


## Chicken Cream Cheese Enchiladas

Makes: 4

**INGREDIENTS:**

1 (8 oz) package cream cheese, softened
3 cups shredded cooked chicken
2 cups shredded Mexican cheese
3 tablespoons unsalted butter
2 cups chicken broth
1 (4 oz) can diced green chiles
8 (6-inch) corn tortillas
3 tablespoons all-purpose flour
1 tablespoon lime juice
Optional: 1/2 teaspoon chili powder
Salt and pepper to taste
Fresh cilantro for garnish

Optional toppings: diced tomatoes, sliced olives, sliced jalapeños, chopped green onions

**DIRECTIONS:**

Preheat the oven to 350°F (175°C) and grease a 9×13-inch casserole dish.

In a bowl, combine half of the cream cheese, chicken, 1 cup of cheese, lime juice, and chili powder (if using). Season to taste.

Fill tortillas with 2-3 tablespoons of the mixture, roll, and place seam side down in the dish.

In a saucepan, melt butter, whisk in flour for 2-3 minutes. Season, add chicken broth, green chiles, and the remaining cream cheese. Cook until thickened.

Pour the green chile sauce over enchiladas and top with the remaining cheese.

Bake for 20-25 minutes. Optionally, broil for a lightly browned top. Allow it to rest before serving. Garnish with cilantro and serve.

**NUTRITION:**

Calories: 576 Carbs: 50g Sodium: 1672mg
Fiber: 4g Protein: 24g


# Disclaimer

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

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

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

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

5. Certain links on the magazine lead to resources located on servers maintained by third parties over whom the PCLinuxOS Magazine has no control or connection, business or otherwise. These sites are external to the PCLinuxOS Magazine and by visiting these, you are doing so of your own accord and assume all responsibility and liability for such action.Material Submitted by UsersA majority of sections in the magazine contain materials submitted by users. The PCLinuxOS Magazine accepts no responsibility for the content, accuracy, conformity to applicable laws of such material.

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


**PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4**

***Uhleash your GIMP & Inkscape skills. Over 160 tutorials. Grab your FREE copy now!***

# Screenshot Showcase

***Posted by parnote, on February 16, 2026, running Xfce.***

# Inspiration & Motivation

# PCLinuxOS Puzzled Partitions

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

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

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

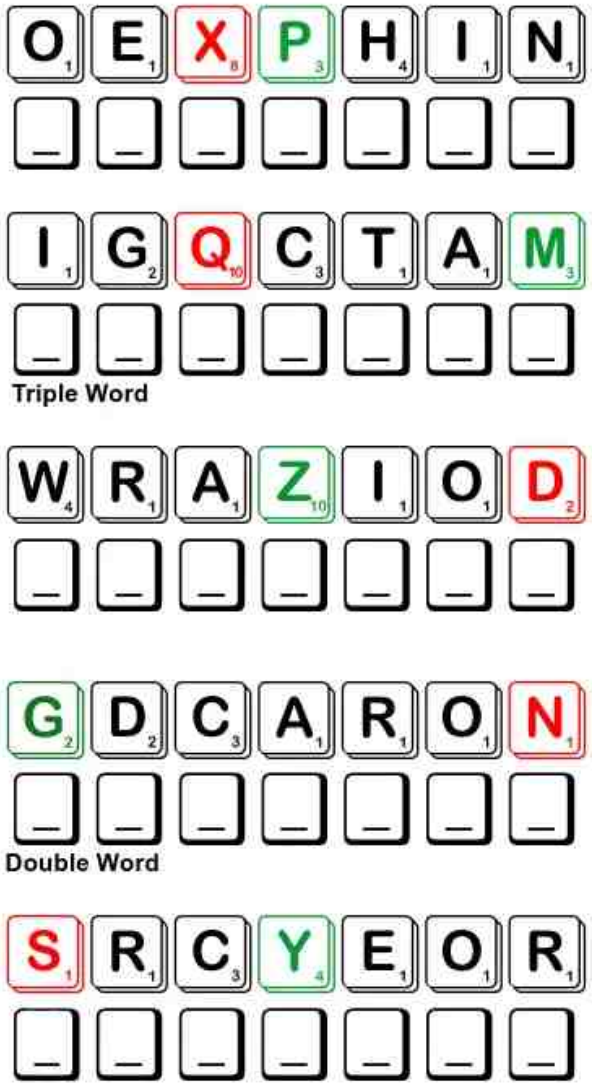
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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 205, average score 144.**

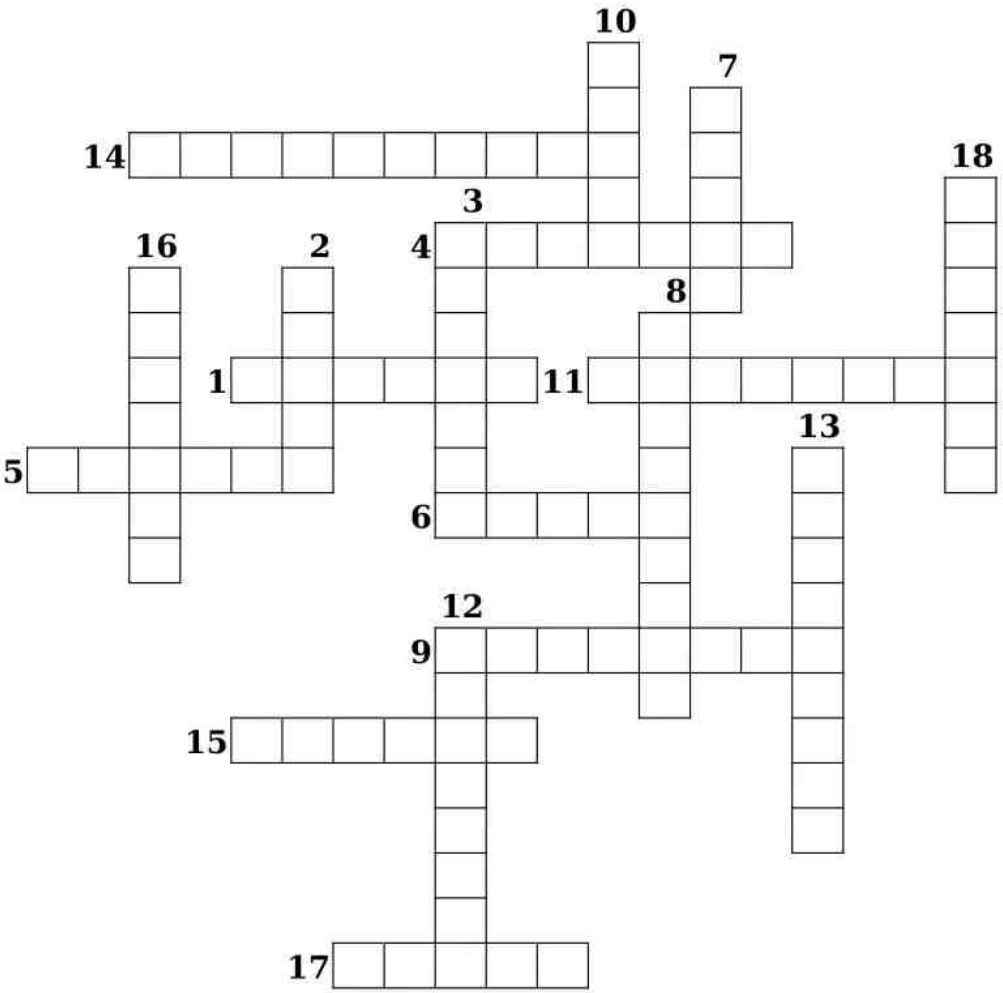
# March 2026 Word Find
# Fantasy

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

| | |
|---|---|
| ALCHEMY | BEWITCHED |
| CAULDRON | CHARMS |
| CHIMERA | CRYSTAL BALL |
| CURSE | DIVINATION |
| DRAGON | DRUID |
| DWARF | ENCHANTMENT |
| FAERIE | GENIE |
| GHOST | GNOME |
| GOBLIN | HOBBIT |
| ILLUSION | LABYRINTH |
| MAGIC | MANTICORE |
| MAZE | MINOTAUR |
| MYTHICAL | PEGASUS |
| PHOENIX | SATYR |
| SORCERY | SPELL |
| SYLPH | UNICORN |
| VALKYRIE | VAMPIRE |
| WEREWOLF | WIZARD |
| WRAITH | YGGDRASIL |
| ZODIAC | ZOMBIE |

**Download Puzzle Solutions Here**

# March 2026 Crossword Fantasy




1. A belt of 12 constellations around the sky through which the Sun, the Moon, and the naked-eye planets move as seen from Earth.
2. One of a fabled race of dwarf-like creatures who live underground and guard treasure hoards.
3. A winged horse in Greek mythology.
4. A legendary bird said to set fire to itself and rise anew from the ashes every 500 years.
5. A small being, human in form, playful and having magical powers.
6. A creature from Greek mythology that is part man and part goat.
7. A member of an ancient Celtic priesthood known for their roles as religious leaders, teachers, judges, and advisors.
8. A place constructed of or full of intricate passageways and dead ends.
9. A monster with the head of a bull and the body of a man.
10. A supernatural creature who does ones bidding when summoned.
11. A female figure in Norse mythology who chooses slain warriors to be taken to Valhalla.
12. Something existing only in stories or imaginary or not real.
13. A huge ash tree in Norse mythology that overspreads the world and binds earth, hell, and heaven together.
14. The art or act of foretelling future events or revealing occult knowledge.
15. An apparition of a living or dead person, or something faint or insubstantial.
16. A fire-breathing female monster in Greek mythology having a lions head, a goats body, and a serpents tail.
17. An imaginary or elemental being that inhabits the air and is mortal but soulless.
18. An imaginary art which aimed to change the baser metals into gold.

**Download Puzzle Solutions Here**

# Mixed-Up-Meme Scrambler

VENAK

CANKS

SNAZAT

PALLAP

What sleeping bags can turn into on the spur of the moment ...

" " _ _ _ _ _ _ _ _ _ _

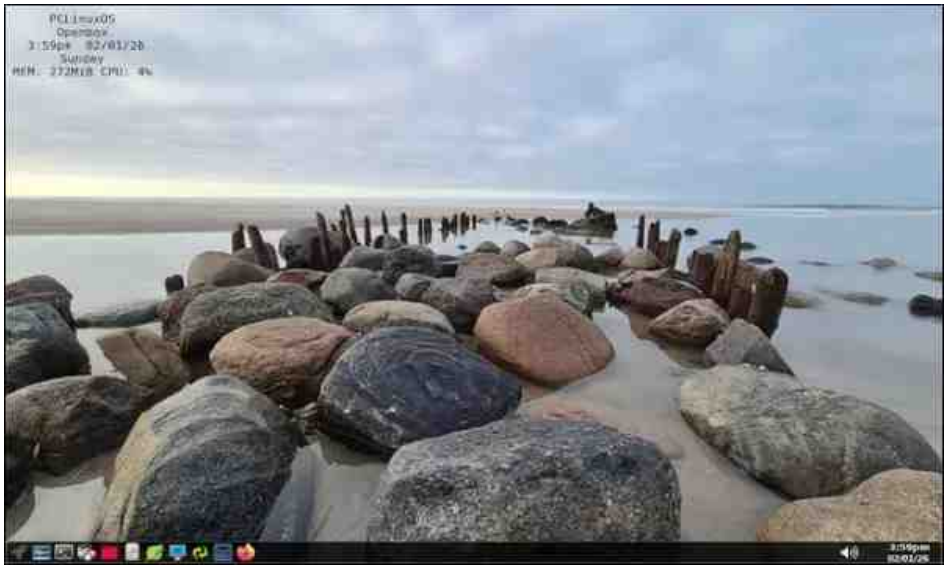
Download Puzzle Solutions Here

# More Screenshot Showcase


*Posted by mutse, on February 12, 2026, running mate.*

*Posted by luikki, on February 10, 2026, running KDE.*

*Posted by francescoinblack, on February 7, 2026, running icewm.*



*Posted by astronaut, on February 1, 2026, running openbox.*