The PCLinuxOS magazine
Volume 226 November, 2025

*Daylight Savings Time Ends Nov. 2, 2025 in the U.S.*

# In This Issue...




The PCLinuxOS magazine





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

This release was made possible by the following volunteers:

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

**Assistant Editor**: Meemaw

**Artwork**: Paul Arnote, Meemaw

**PDF Layout**: Paul Arnote, Meemaw

**HTML Layout**: tbs

**Staff**:

YouCanToo David Pardue

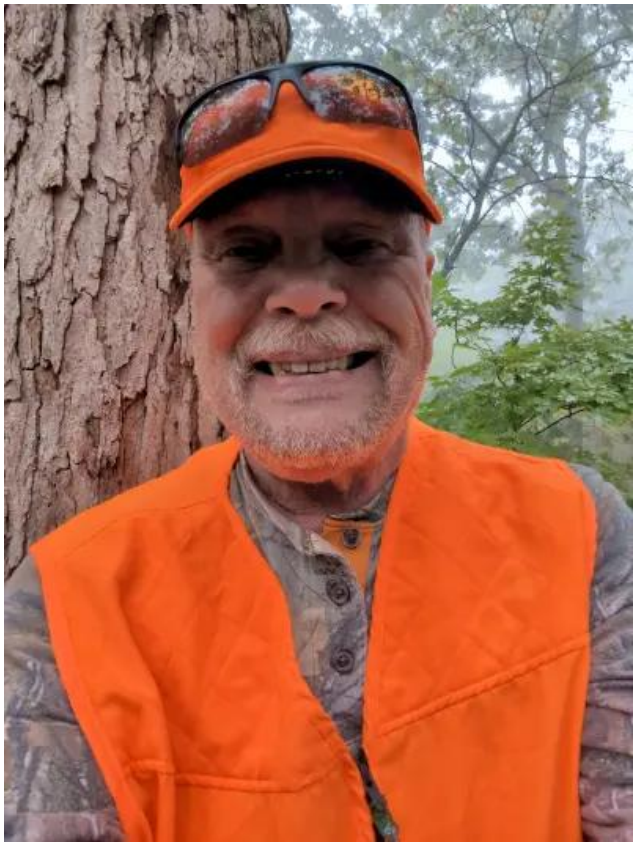
Alessandro Ebersol

**Contributors**:

# From The Chief Editor's Desk

On November 2, the 2025 “version” of Daylight Savings Time ends, at least in the U.S. Hallelujah!

I am NOT a fan of Daylight Savings Time, just in case that wasn’t apparent. You cannot make a longer day by chopping an hour off of the beginning of the day, and tacking it on at the end. When it’s all said and done, a day is a day is a day. 24 hours. Period. That’s it. So stop messing with the freakin’ clocks!



If you want more hours of sunlight, get yo’ assets out of bed earlier … like when the sun comes up. If you sleep in, the wasted hours of daylight are solely on YOU. You snooze, you lose! It’s really that simple.

Oh, over the years, they’ve touted the “benefits” of DST. It was made a “permanent” albatross here in the U.S. during the oil crisis in the late 70s and early 80s. We were told that it would lessen energy usage, except, there really was no discernable difference in energy usage when they went back and looked at the numbers.

We were told that farmers would have more hours of daylight to work in their fields, as if they don’t already work hard and long enough. Except, farmers (especially dairy farmers, who deal with dairy cattle, which have NO idea about a clock or our manipulations of that said clock) already maximize their available work hours by … wait for it … getting up when the sun comes up. As for those cattle, they expect to be milked every morning and every evening, without any regard towards the positioning of the hands on a human-devised clockface. The time is the same to those cattle, whether those hands on that human-devised clock read 0400 or 0500 or 0600. The circadian rhythms of the cows are regulated by … again, wait for it … when the sun comes up and when the sun goes down. That makes the cows seem a LOT more intelligent than their human “overlords.”

At least with the end of DST, there are a LOT less physical ailments related to the time manipulation than there is when we lose an hour of sleep in the spring. Getting that extra hour of sleep in the fall when we turn the clocks back to “regular” time is welcomed by most people.

However, in the spring, when we typically switch to DST, there are increases in heart attacks, strokes, depression and anxiety, and sleep disorders, along with a 6% increase in fatal automobile crashes (most likely related to the lost hour of sleep). Lots of people suffer cognitive impairment, most likely associated with the shortened amount of sleep. They have also found that DST can cause metabolic disturbances, due to the change in sleep patterns, which can lead to weight gain and other metabolic disorders.

I can tell you, as a retired healthcare professional, that there are negative physical manifestations of messing with the time. Every spring, we would actually see all sorts of physical problems for the first couple of weeks after the time change. Without a doubt, we usually saw an increase in heart attacks coming through the Emergency Room doors.

There are some lawmakers who want to make DST permanent, all year long. While it would end the biannual “dance” we make with the clock hands (and thus, relieve the physical stresses associated with the twice-a-year time

change), it still “embraces” the debunked idea that the time change helps lessen energy usage, along with every other touted “benefit” of DST.

I’m actually more in favor of staying on “regular” time all year long. Making a large number of people alter their routines and sleep patterns in the name of some “benefits” that have never been proven to exist is just asinine.

**********

This month’s cover image is by Pixabay artist Gerd Altmann. His image of clocks in the style of Salvador Dali exemplifies the biannual time dance we perform with our clocks.

**********

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



**Like Us On Facebook!**
**The PCLinuxOS Magazine**
**PCLinuxOS Fan Club**

# Screenshot Showcase

***Posted by YouCanToo, on October 8, 2025, running KDE***

# ICYMI: Perplexity AI Launches Comet Browser

**by Paul Arnote (parnote)**

Google plans to begin testing its recently announced verification scheme for Android developers in the coming weeks, but there's still precious little information on how the process will work. F-Droid, the free and open source app repository, isn't waiting for the full rollout to take a position. In a blog post, **F-Droid staff say that Google's plan to force devs outside Google Play to register with the company threatens to kill alternative app stores like F-Droid**, according to an article from ArsTechnica. F-Droid has been around for about 15 years and is the largest source of free and open source software (FOSS) for Android. Because the apps in F-Droid are not installed via the Play Store, you have to sideload each APK manually, and Google is targeting that process in the name of security. However, there's a LOT of confusion surrounding this latest move by Google with the Android ecosystem. According to an article from Android Police, First and foremost, Google clarifies that it is not killing or doing away with sideloading on Android with this move. Instead, it says, "our new developer identity requirements are designed to protect users and developers from bad actors, not to limit choice. We want to make sure that if you download an app, it's truly from the developer it claims to be published from, regardless of where you get the app." Still, it does not address the fact that developers must pay Google for identity verification. Plus, they must accept the company's terms and conditions and upload personally identifiable documents. Meanwhile, you can read F-Droid's full take on the situation here. To say that this issue is "resolved" would be overly optimistic and simplistic. We, the users of Android, will have to sit back and see how this all shakes out.

**A viral app called Neon, which offers to record your phone calls and pay you for the audio so it can sell that data to AI companies, has rapidly risen to the ranks of the top-five free iPhone apps since its launch last week**, according to an article from TechCrunch. The app already has thousands of users and was downloaded 75,000 times yesterday alone, according to app intelligence provider Appfigures. Neon pitches itself as a way for users to make money by providing call recordings that help train, improve, and test AI models. But Neon has gone offline, at least for now, after a security flaw allowed anyone to access the phone numbers, call recordings, and transcripts of any other user, TechCrunch can now report.

**Security researchers have uncovered critical vulnerabilities in Tile's location trackers that could allow stalkers to covertly monitor users by exploiting the devices' lack of encryption**, according to an article from eSecurity Planet. The flaws highlight longstanding privacy concerns surrounding Bluetooth-enabled trackers, which are marketed as tools to help people locate lost items but can be exploited for invasive surveillance. According to researchers from the Georgia Institute of Technology, the way Tile devices communicate leaves owners exposed to stalking. Unlike Apple AirTags and

Samsung SmartTags, which rotate both unique identifiers and MAC addresses, Tile only rotates the unique identifier, allowing adversaries to fingerprint and track a tag indefinitely. There's an additional informative article from Wired that goes into a deeper explanation.

**Perplexity AI on October 2 announced that its artificial intelligence-powered web browser Comet is available worldwide, and will be free to users**, according to an article from CNBC. The Comet browser is designed to serve as a personal assistant that can search the web, organize tabs, draft emails, shop and more, according to Perplexity. The startup initially launched Comet in July to Perplexity Max subscribers for $200 a month, and the waitlist has ballooned to "millions" of people, the company said. Perplexity's decision to provide Comet for free could help it attract more users as it works to fend off rivals like Google, OpenAI and Anthropic that have their own AI browser offerings.

**Web browsers collect a lot of data and share it with the sites we visit, so if you're concerned about your privacy, it's worth wondering which browsers are best for keeping our online habits to ourselves**, according to an article from Lifehacker. Whether you're an activist concerned about surveillance, someone doing research in a country where your topic can get you in trouble, or simply a person who doesn't want spying eyes on their search history, using a more private browser can be one of the simplest steps you can take towards less worry. The author spoke to William Budington, a Senior Staff Technologist on The Electronic Frontier Foundation's (EFF) Public Interest Team, and Janet Vertesi, an Associate Professor of Sociology at Princeton University who publishes extensive work on human-computer interaction and online privacy. They had subtly different opinions on which browsers are best for your privacy, but they definitively agreed on one thing: It's not Chrome.

AI has been used to paraphrase deadly proteins in ways that slipped past DNA security safeguards. **A Microsoft-led team found that some AI-crafted ricin variants evaded detection entirely**, according to an article from eWeek. In a study detailed in the journal Science, the researchers tested two major companies' biosecurity screening techniques and found that up to 100% of the AI-generated ricin-like proteins evaded detection. The finding exposes how existing filters can fail when tested against AI-designed toxins. Around October 2023, Microsoft's Eric Horvitz and Bruce Wittmann began a red-teaming study to probe weaknesses in DNA biosecurity safeguards. Borrowing a term from military strategy, the exercise was designed to mimic how a malicious actor might try to exploit artificial intelligence to bypass security controls. The team used open-source protein design models to digitally reformulate 72 proteins under legal control, including ricin, botulinum, and Shiga toxins. In total, they created more than 70,000 synthetic DNA sequences that could code for variant forms of these toxins. None of the sequences were manufactured in the lab, but they were run through the same biosecurity screening software used by DNA synthesis companies to flag dangerous orders.

**Asahi Group Holdings has reported a cyberattack on its domestic operations in Japan**, according to an article from Just Drinks. The Peroni beer and Nikka whisky owner said the incident happened earlier on September 29. In a short statement sent to Just Drinks just after midday, Asahi said its Japanese operations had seen a "system failure." "On September 29, around 7:00 a.m. Japan time, Asahi Group experienced a system failure due to the impact of a cyberattack on operations in Japan. At this

time, there is no estimated timeline for recovery. There has been no confirmed leakage of personal information or other data to external parties. The system failure is currently limited to our operations within Japan." Reuters reported the company had stopped orders and shipments as a result of the incident.

**Intel Corp., the embattled chipmaker now backed by the US government, introduced new products and manufacturing technology that are central to its turnaround bid**, according to an article from Bloomberg. The company announced Thursday that its Panther Lake processor designs are in full production and will go on sale in laptops early next year. The new chips are made with 18A technology, which Intel says offers advantages that none of its competitors can match yet. The unveiling follows a furious six-month stretch for Chief Executive Officer Lip-Bu Tan. After taking the job in mid-March, he's tried to shake up Intel while also seeking outside help. The US government has become the chipmaker's biggest investor as part of an unconventional deal brokered by the White House, and Nvidia Corp. and SoftBank Group Corp. have acquired multibillion-dollar stakes.

**On Friday, Oct. 3, Discord announced that a third-party service provider it uses for customer service efforts suffered a breach**, according to an article from Lifehacker. It warned a "limited number of users" who had communications with certain Discord teams were affected, though the "unauthorized party" did not gain access to any Discord networks directly. In that initial announcement, Discord said a number of user data types might have been stolen. That included their names, usernames, email addresses, billing information, last four digits of credit cards, purchase histories, IP addresses, messages with Discord service agents, and "limited corporate data," such as training materials and internal presentations. While all of this information is sensitive, it unfortunately isn't surprising to see it as part of a breach like this. However, Discord also revealed that the hackers may have also gained access to a "small number" of government ID images, including driver's licenses and passports. As it turns out, that "small number" turned out to be 70,000. Discord confirmed as much to The Verge on Wednesday. If you were among these affected users, Discord will have reached out to you via email.


**Take note, Nvidia: OpenAI is tightening its grip on the AI economy. With a new partnership, the company is targeting the single biggest bottleneck in its supply chain: the chip**, according to an article from eWeek. According to a press release published Monday, OpenAI has struck a deal with Broadcom to co-develop its first in-house AI processor. The move is part of an effort to reduce reliance on third parties, such as Nvidia, and exert greater control over the infrastructure that drives its models. "Partnering with Broadcom is a critical step in building the infrastructure needed to unlock AI's potential," OpenAI CEO Sam Altman said in a statement. "Developing our own accelerators adds to the broader ecosystem of partners, all building the capacity required to push the frontier of AI to provide benefits to all humanity." This news comes just a week after OpenAI signed a multi-year partnership with chipmaker AMD to supply the processors powering its next-generation AI systems.

**SimonMed Imaging has revealed that a data breach resulting from a ransomware attack has impacted more than 1.2 million individuals**, according to an article from Security Week. According to its website, SimonMed Imaging is one of the largest medical imaging providers and physician radiology practices in the US, with more than 170 facilities across 10 states. The Arizona-based healthcare organization learned in late January 2025 that one of its vendors had been breached, and an investigation conducted by SimonMed showed that its own network had also been hacked. The probe revealed that hackers had access to SimonMed systems between January 21 and February 5, and they managed to steal information such as name, address, date of birth, health insurance information, driver's license number, government-issued ID, SSN, financial account number, authentication credentials, and a wide range of medical information.

**In August 2025, cybersecurity researchers uncovered a sophisticated hacking campaign exploiting Microsoft Edge's Internet Explorer (I.E.,) mode to compromise users' devices**, according to an article from eSecurity Planet. By leveraging social engineering and

zero-day vulnerabilities within IE's outdated Chakra JavaScript engine, threat actors successfully bypassed modern browser protections. This discovery highlights the persistent risks of maintaining legacy compatibility features in today's rapidly evolving digital landscape. Microsoft Edge's IE mode was originally developed to provide compatibility for older web applications and technologies that relied on outdated frameworks such as ActiveX, Silverlight, or Flash. Many enterprises, government portals, and industrial systems still depend on these legacy components, making full deprecation impractical. However, attackers have now weaponized this compatibility feature to bypass modern browser security protections. In this campaign, adversaries combined social engineering and zero-day exploits to manipulate unsuspecting users into reloading web pages in IE mode.

**U.S. cybersecurity company F5 disclosed that nation-state hackers breached its systems and stole undisclosed BIG-IP security vulnerabilities and source code**, according to an article from Bleeping Computer. The company states that it first became aware of the breach on August 9, 2025, with its investigations revealing that the attackers had gained long-term access to its system, including the company's BIG-IP product development environment and engineering knowledge management platform. F5 is a Fortune 500 tech giant specializing in cybersecurity, cloud management, and application delivery networking (ADN) applications. The company has 23,000 customers in 170 countries, and 48 of the Fortune 50 entities use its products. BIG-IP is the firm's flagship product used for application delivery and traffic management by many large enterprises worldwide. F5 has released a Security Incident "report" on its website.

Microsoft ended official support for Windows 10 on October 14, 2025, but the operating system will continue to function. **While major software vendors and game studios will eventually leave the platform behind, users who are concerned can begin planning alternatives immediately, and Commodore is now offering an escape route**, according to an article from TechSpot. The official Commodore Twitter account recently promoted Vision OS as a potential alternative to Microsoft's ecosystem. Commodore OS Vision 3.0 is a Linux-based platform specifically designed to protect users from what the company describes as Big Tech's monopolistic practices, constant digital noise, and pervasive surveillance. The operating system can be downloaded for free, with Commodore providing detailed installation instructions. It is also included with the Commodore 64X PC, a modern reinterpretation of the classic computing brand featuring recent x86 CPUs and contemporary hardware components. I don't know about you, but I wasn't aware that this company was even still around!!!

**Google has released an urgent security update for its Chrome browser, addressing a serious vulnerability that could allow attackers to take control of users' systems simply by visiting a malicious website**, according to an article from eSecurityPlanet. Chrome versions prior to 141.0.7390.107/.108 for Windows and Mac and 141.0.7390.107 for Linux are impacted. The Hong Kong CERT team stated, "A remote attacker could exploit this vulnerability to trigger remote code execution on the targeted system." The vulnerability (CVE-2025-11756) affects Chrome's Safe Browsing feature, a key layer of defense designed to protect users from phishing sites and malware downloads. It was discovered by a researcher in September 2025, and reported to Google. At the time of publication, Google has not released detailed technical details of this vulnerability. Because Safe Browsing runs with elevated privileges, a successful exploit could bypass Chrome's sandbox protections—potentially granting full access to the underlying operating system.


**A major worldwide outage hit several of the biggest websites and apps on the morning of October 20, 2025, with major names such as Snapchat, Roblox, Canva, and Duolingo all suffering downtime**, according to an article from TechRepublic. Amazon Web Services (AWS), the cloud provider behind many of these platforms, is at fault for the disruption. It began reporting faults across multiple AWS services in the US-EAST-1 region at midnight Pacific Time, with the underlying DNS issue fully mitigated by 3AM PDT. However, three hours later, Amazon reported new API and connectivity issues, with further investigation underway to resolve them. Even after mitigation efforts, services running on AWS are expected to remain unstable for a few hours due to traffic spikes and other technical factors. Beyond the thousands of apps, games, and websites affected, some of Amazon's own services also went down during the outage. Amazon's retail site was unavailable for several hours, as was its Ring doorbell system. Delivery drivers in the UK reported that Amazon warehouses were unable to sign off on packages due to technical faults.

**In a very public, very awkward lesson on the difference between "solving" a problem and simply "finding" the answer, OpenAI's latest model, GPT-5, has stirred up controversy**, according to an article from eWeek. Top researchers at the company took a premature victory lap on social media, claiming the AI had cracked a set of notoriously difficult mathematical riddles. The celebration, however, was short-lived, earning the AI giant a stern rebuke and a fresh wave of industry ridicule. Mathematician Thomas Bloom, who runs the Erdős Problems website, quickly poured cold water on the celebrations. Responding on X, Bloom wrote, "Hi, as the owner/maintainer of http://erdosproblems.com, this is a dramatic misrepresentation. GPT-5 found references, which solved these problems, that I personally was unaware of." He clarified that when a problem is marked as "open" on his website, it simply means he hasn't seen a paper that solves it, not that the problem is still unsolved. In other words, GPT-5 didn't actually produce new proofs; it merely discovered papers that already contained the solutions. Even Google DeepMind's CEO, Demis Hassabis, chimed in, calling the situation "embarrassing." And Meta's AI chief Yann LeCun took a sharper jab, quipping, "Hoisted by their own GPTards."

For all the discoveries we're making of faraway galaxies, we're still struggling to fully understand our own galaxy, the Milky Way. For example, researchers have known for decades of an odd concentration of gamma rays near the center of the Milky Way, although they weren't sure where the high-energy light was coming from. **A new study proposes an entirely new perspective — that the light may actually be coming from neutron stars, as astronomers have suspected**, according to an article from Gizmodo. If not, however, this could be the "first proof" of dark matter, according to the paper, published recently in Physical Review Letters. Given the evolution of the Milky Way, the researchers argue that the gamma ray excess most likely emerged from the collision of dark matter particles, the researchers claim.

**NASA has officially confirmed that Earth has gained a new, albeit temporary, cosmic companion — a "quasi-moon" named 2025 PN7**, according to an article from Southern Digest (and widely reported on by multiple media outlets). First discovered by the University of Hawaii during a telescope survey earlier this year, the asteroid travels in near synchronization with Earth's orbit around the Sun. While it doesn't qualify as a true moon, its unique movement pattern means it acts like a shadow companion, orbiting the Sun alongside

us for decades. According to NASA's calculations, this celestial partner will likely remain in Earth's neighborhood until 2083, making it one of the longest-staying quasi-moons ever recorded. Measuring an estimated 18 to 36 meters wide — roughly the height of a four- to eight-story building — 2025 PN7 is small but significant, adding a new chapter to humanity's understanding of near-Earth objects. Unlike the Moon that we see in the night sky, which is gravitationally bound to Earth, a quasi-moon follows an orbit around the Sun, not Earth itself. However, its orbit is synchronized in such a way that it appears to loop around Earth as both move through space. NASA compares the behavior of a quasi-moon to that of "a runner on a nearby lane", keeping pace without ever colliding or falling behind. 2025 PN7's orbit has been in step with Earth's for nearly six decades, and scientists predict that it will maintain this synchronized dance for another half-century.

Running out of storage space forces impossible choices: delete old files, pay monthly cloud subscriptions that add up fast, or buy expensive SSDs that cost ten times more per gigabyte than traditional hard drives. **The Seagate 20TB external hard drive just dropped to $229 on Amazon (down from $499) and puts it at barely over one cent per gigabyte**, according to an article from Gizmodo. This is an all-time low for this much capacity, and for context, cloud storage typically runs around $10 per month for just 2TB, meaning you'd spend $100 annually for a tenth of what this drive offers as a one-time purchase. If you're backing up years of photos, managing video projects, archiving work files, or hoarding a media library, this drive delivers more practical storage than any cloud service or SSD at this price point.

mRNA-based Covid vaccines from Pfizer-BioNTech or Moderna may have an unexpected benefit for cancer patients who undergo immunotherapy. **A new study suggests that these vaccines might boost the effects of immunotherapy drugs, perhaps by alerting the immune system and helping direct immune cells to attack tumors**, according to an article from STAT News. That's in addition to helping protect against Covid, which can be particularly important for cancer patients, who can sometimes have weakened immune systems. The study found that advanced cancer patients who received a Covid vaccine within 100 days before taking an immunotherapy drug during the pandemic lived longer than patients who did not, in a retrospective analysis. Researchers from MD Anderson Cancer Center presented the study at the European Society for Medical Oncology conference in Berlin on Sunday.

*Image by Md Shahin from Pixabay*

**A new review suggests that vitamin D supplements may help protect the ends of our chromosomes, known as telomeres, which play a vital role in slowing the aging process**, according to an article from Science Daily. This finding has raised hopes that the "sunshine vitamin" could support longer-lasting health. Researchers found that taking 2,000 IU (international units, a standard measure for vitamins) of vitamin D daily helped preserve telomeres -- the tiny protective caps on our DNA that function like the plastic tips on shoelaces, preventing damage each time a cell divides. Each of our 46 chromosomes is capped with a telomere that becomes shorter every time a cell replicates. When these structures get too short, cells stop dividing and eventually die. Shortened telomeres have been linked to major age-related diseases such as cancer, heart disease, and osteoarthritis. Factors like smoking, chronic stress, and depression can speed up this shortening process, while inflammation in the body also contributes to it.

**OpenAI announced on October 20, 2025, that it's rolling out a new internet browser called Atlas that integrates directly with ChatGPT**, according to an article from Wired (and widely reported on by multiple media outlets). Atlas includes features like a sidebar window people can use to ask ChatGPT questions about the web pages they visit. There's also an AI agent that can click around and complete tasks on a user's behalf. "We think that AI represents a rare, once-a-decade opportunity to rethink what a browser can be about," OpenAI CEO Sam Altman said during a livestream announcing Atlas. "Tabs were great, but we haven't seen a lot of browser innovation since then." Atlas debuts as Silicon Valley races to use generative AI to reshape how people experience the

internet. Google has also announced a plethora of AI features for its popular Chrome browser, including a "sparkle" button that launches its Gemini chatbot. Chrome remains the most used browser worldwide. OpenAI says the Atlas browser will be available starting today for ChatGPT users globally on macOS. Windows and mobile options are currently in the works. Atlas is free to use, though its agent features are reserved for subscribers to OpenAI's ChatGPT Plus or ChatGPT Pro plans.

**Google announced research that shows — for the first time in history — that a quantum computer can successfully run a verifiable algorithm on hardware, surpassing even the fastest classical supercomputers (13,000x faster)**, according to an article from Google's Technology blog. It can compute the structure of a molecule, and paves a path towards real-world applications. Today's advance builds on decades of work, and six years of major breakthroughs. Back in 2019, Google demonstrated that a quantum computer could solve a problem that would take the fastest classical supercomputer thousands of years. Then, late last year (2024), Google's new Willow quantum chip showed how to dramatically suppress errors, solving a major issue that challenged scientists for nearly 30 years. Today's breakthrough moves Google much closer to quantum computers that can drive major discoveries in areas like medicine and materials science.



Image by airinai125 from Pixabay

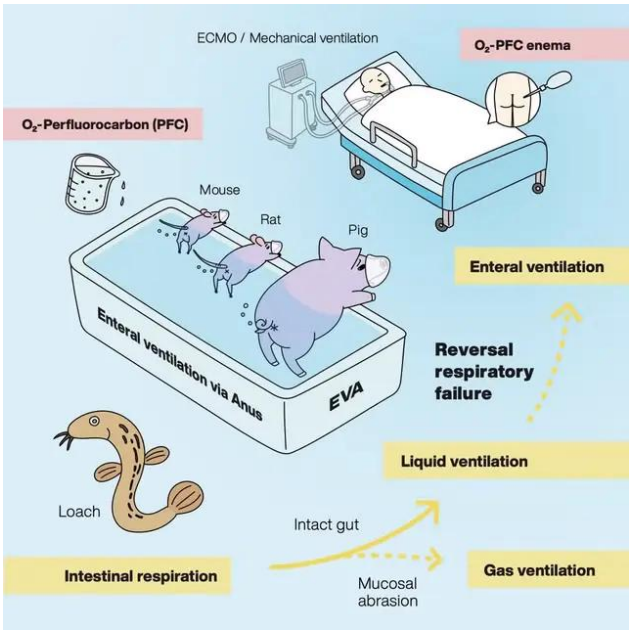
**Researchers at the University of Maryland have identified the gene responsible for a rare wheat variety that develops three ovaries in each flower instead of just one**, according to an article from SciTechDaily. Because every ovary can grow into a grain, this finding could greatly increase the amount of wheat produced per acre. The discovery was detailed in the Proceedings of the National Academy of Sciences on October 14, 2025. The unusual three-ovary trait was first found in a naturally occurring mutant of common bread wheat, but scientists did not initially know what caused it. To uncover the genetic difference, the Maryland team created a precise map of the mutant wheat's DNA and compared it with that of ordinary wheat. Their analysis revealed that a normally inactive gene, known as WUSCHEL-D1 (WUS-D1), had been activated. When WUS-D1 turns on early during flower formation, it enlarges the floral tissue and allows the plant to produce additional female organs, such as pistils or ovaries.

**The Nobel Prize in Physics has been awarded to John Clarke, Michel H. Devoret and John M. Martinis for their work on quantum mechanics that is paving the way for a new generation of very powerful computers**, according to an article from the BBC. "There is no advanced technology used today that does not rely on quantum mechanics, including mobile phones, cameras... and fibre optic cables," said the Nobel Committee. The announcement was made by the Royal Swedish Academy of Sciences at a news conference in Stockholm, Sweden. "To put it mildly, it was a surprise of my life," said Professor John Clarke, who was born in Cambridge, UK and now works at the University of California in Berkeley. Michel H. Devoret was born in Paris, France and is a professor at Yale University

while John M. Martinis is a professor at University of California, Santa Barbara. The three winners will share prize money of 11 million Swedish kronor (£872,000).

**The genes we inherit may have a subtle influence over whether we experiment with and make a habit of using cannabis**, according to an article from Science Alert. A team led by researchers from Western University in Canada, the University of California, San Diego (UC San Diego), and personal genomics and biotechnology company 23andMe compared the full genomes of 131,895 individuals with self-reported frequency of cannabis use. In addition to identifying variations in two key genetic sequences associated with cannabis use, the study linked the same genetic patterns to more than a hundred other physical and mental health traits, providing clues on how drug use relates to our wellbeing. Numerous factors can affect whether an individual uses drugs for self-medication or recreational purposes, from where they live to how much money they have. Genetics often has a more indirect impact on our habits, making some prone to experimental or frequent use despite risks of ongoing harm.




*Institute of Science Tokyo*

**A seemingly outlandish method to deliver oxygen rectally – one of the winners of the 2024 "Ig Nobel" satirical science prize – may one day actually help lung disease patients, after achieving a key step in clinical trials**, according to an article from The Independent. The technique was first demonstrated in 2021 by Japanese researchers, who showed in experimental pig models that oxygen could be delivered to the body via the rectum in gas form. An enema-like process delivers super-oxygenated liquid to the large intestine, where the life-supporting gas is absorbed into the bloodstream. While this method of rescuing people with blocked airways led the research team to win a parody award, it might not be a joke after all.

**Scientists are reporting the first compelling evidence in people that cognitive training can boost levels of a brain chemical that typically declines with age**, according to an article from NPR. A 10-week study of people 65 or older found that doing rigorous mental exercises for 30 minutes a day increased levels of the chemical messenger acetylcholine by 2.3% in a brain area involved in attention and memory. The increase "is not huge," says Étienne de Villers-Sidani, a neurologist at McGill University in Montreal. "But it's significant, considering that you get a 2.5% decrease per decade normally just with aging." So, at least in this brain area, cognitive training appeared to turn back the clock by about 10 years.

**AI "slop" has come for herbalism, a study published by a leading AI-detection company has found**, according to an article from The Guardian. Originality.ai, which offers its tools to universities and businesses, says it scanned 558 titles published in Amazon's herbal remedies subcategory between January and September this year, and found 82% of the books "were likely written" by AI. "This is a damning revelation of the sheer scope of unlabelled, unverified, unchecked, likely AI content that has completely invaded [Amazon's] platform," wrote Michael Fraiman, author of the study. "There's a huge amount of herbal research out there right now that's absolutely rubbish," said Sue Sprung, a medical herbalist in Liverpool. "AI won't know how to sift through all the dross, all the rubbish, that's of absolutely no consequence. It would lead people astray." One of the apparently AI-written books, Natural Healing Handbook, is a No 1 bestseller in

Amazon's skincare, aroma therapies and herbal remedies, subcategories. Its introduction touts the book as "a toolkit for self-trust", urging readers to "look inward" for solutions. Natural Healing Handbook's author is named as Luna Filby, whose Amazon page describes her as a "35-year-old herbalist from the coastal town of Byron Bay, Australia" and founder of the brand My Harmony Herb. Sarah Wynn, the founder of Wildcraft Journal, calls the book a "resource and an inspiration". However, neither Luna Filby, My Harmony Herb, Wildcraft Journal or Sarah Wynn appear to have any online presence beyond the Amazon page for the book – an indication, said Fraiman, that they may not exist. The Guardian could find no evidence of the pair. Originality.ai's tool flagged available samples of the text as AI-generated with "100% confidence".



## Screenshot Showcase


*Posted by Texstar, on October 3, 2025, running KDE*

# PCLinuxOS Recipe Corner


## *Homemade Hamburger Help Basic Mix – with some basic recipes*

**BASE MIX:**

2 cups nonfat dry milk
1 cup corn starch
1/4 cup beef bouillon powder
2 T onion flakes
1 tsp dried basil
1 tsp dried thyme
1 tsp black pepper
2 T dried parsley
1 T garlic powder

Measure all ingredients into a Ziploc Bag. Shake well, transfer to a vacuum seal bag, seal and store for up to a year. To use, see recipes below, each recipe calls for 1/2 c. of the mix above.

**Chili Mac:**
1 lb. ground beef or turkey,
browned and drained
1 C. water
1/2 C. macaroni noodles (uncooked)
2 cans chopped tomatoes
1 T. chili powder
1/2 C. mix

Combine all and simmer for 20 minutes or until macaroni is cooked.

**Stroganoff:**
1 lb. ground beef or turkey,
browned and drained
2 C. water
1/2 C. mix
2 C. uncooked egg noodles
1/2 C. sour cream

Combine all except sour cream. Simmer for 20 minutes or until noodles are tender. Stir in sour cream and serve.

(Alternatively, here's how I prefer to make mine- Heat a Large skillet over medium heat, place ground meat in pan to brown, when halfway cooked add 1/2 a small onion diced, 1/2 c diced bell pepper (red or green or both) until meat is no longer pink. Add Water & Mix, whisk to combine and break up any chunks. Add noodles. Cover & cook 15-20 minutes or until noodles are tender, Stir in Sour cream & Serve)

**Potato Beef Casserole:**
1 lb. ground beef or turkey, browned
and drained
3/4 C. water
6 potatoes, peeled and thinly sliced
1 C. frozen mixed veggies
1/2 C. mix

Combine all and simmer, covered, until potatoes are tender, about 30 minutes, stirring occasionally. Remove cover and cook until excess water has evaporated.

**Lasagna:**
1 lb. ground beef or turkey,
browned and drained
1/2 C. mix
1 onion, chopped
2 C. water
16 oz. tomato sauce
3 C. lasagna noodles, uncooked, broken in bits
1/4 C. parmesan cheese
2 C. mozzarella cheese, shredded

Combine all except mozzarella in a large skillet. Bring to a boil, let simmer for 15 minutes or until noodles are cooked. Top with mozzarella. Turn off heat and let cheese melt.

# DOSBOX Pure: Run Your Old DOS Games On PCLinuxOS

**by Agent Smith (Alessandro Ebersol)**

**DOSBOX on steroids: DOSBox Pure**


So, friends, the famous Disk Operating System, also known as PC-DOS, IBM-DOS, or MS-DOS, depending on who sold the computer/system, was one of the most famous operating systems that ever existed. And it still exists. DOS is still being developed, such as FreeDOS, and there is still equipment, whether embedded electronics, handhelds, or industrial computers that still run on the DOS standard.

We cannot estimate, either humanly or with AI (and I tried), how many programs have been made for DOS, and thanks to the almost unlimited library of programs for this operating system, it is still very popular among computer users. I bet that you, reading this now, have a favorite DOS game that you occasionally play to satisfy your urge to game and remember the good old days (when Microsoft still had some competence).

The options we have today to revive old DOS programs are DOSEMU and DOSBOX. DOSEMU is somewhat complicated to get working, so that leaves us with DOSBOX.

**DOSBOX: Good enough, but not quite good enough**


DOSBOX is a very easy-to-use application, it is stable, and it runs many DOS programs. However, despite being relatively easy and not very complex, it does have some issues:

- There are settings to configure, and they are quite complicated, often requiring a graphical front-end due to their complexity.

- Development stopped at version 0.74.3 in 2019, and since then no improvements to the main project have been presented. Several forks have appeared, which we will look at next.

- There are not many options with DOSBOX for running programs with more advanced features, such as 3D acceleration.

As I mentioned above, the original DOSBOX stopped at version 0.74.3, but numerous forks have emerged. Namely:

- DOSBox Staging
- DOSBox-X
- DOSBox SVN Daum (discontinued)
- DOSBox Turbo (Android)
- DOSBox Pure

**DOSBox Pure: Many advanced features in one emulator**

DOSBox Pure is an innovative fork of the original DOSBox emulator, designed specifically to enhance the emulation experience of old DOS-based software. While DOSBox is widely appreciated for its ability to run DOS software on modern operating systems, DOSBox Pure elevates the experience by introducing features focused on ease of use, compatibility, and improved performance.

Initially developed as a Retro Arch core, it was recently released as a standalone program, the Unleashed version. It was this version that I packaged and tested, and now I bring you an overview of some of its features.

One of the standout features of DOSBox Pure is its goal of simplifying the configuration process for users. Unlike the original DOSBox, which often requires significant configuration for games to run smoothly, DOSBox Pure simplifies this with automatic game configuration detection. Simply drag the game ISO or the folder with the game already installed into the main DOSBox Pure window, and it will do the rest, asking a minimum of questions about the game and then running it.

DOSBox Pure also improves compatibility with modern hardware. While classic DOSBox sometimes struggles with modern peripherals, Pure integrates improved mouse and joystick handling, ensuring a more seamless experience when running games that rely on these inputs. DOSBOX Pure has support ready for Xbox 360 joysticks, a current standard. In addition, the emulator supports high-resolution scaling and shading effects, which enrich the visual presentation of older titles without compromising their nostalgic aesthetic. It is possible to run games compatible with accelerated hardware, such as 3DFx, at resolutions up to 4K.

**Features**

● Load games from ZIP Files

You can have your games, with the entire directory structure compressed as ZIP files, and simply drag them to the DOSBox Pure main screen. The emulator will ask which program to run and will then execute it.

● Store Modifications in a Separate Backup Files

Changes made to a loaded ZIP file will be stored as a separate ZIP file in the saves directory. If a game is loaded directly without using a container such as ZIP or ISO, the saves directory will not be used.

● Mount Disk Images from Inside ZIP Files

CD images (ISO or CUE) and floppy disk images (IMG/IMA/VHD/JRC/TC) can be mounted directly from within ZIP files, eliminating the need for complicated commands to mount ISO images.

The system will automatically mount the first disk image found as drive A: or D:.

Additional disks can be loaded or swapped using the Start menu.

● Start Menu


This is the first screen that appears after loading a game. It provides a joystick-controlled list of all executable files for the loaded game. It also allows you to load new content and switch the inserted disk or CD.

Using the tabs at the bottom, you can view the Control Mapper, System Settings, and, while a game is running, access the Virtual Keyboard.


While a game is running, you can open the menu again by pressing CTRL+F12 or L3 on the controller (usually by pressing the left analog stick). The keyboard shortcut can be modified in System Settings, and the controller button can be changed in the Control Mapper.

Since DOSBOX Pure is a software with an emphasis on ease of use and intuitiveness, configuring it is very simple.

**How to configure DOSBOX Pure**

On the main screen, the start menu, look for the SYSTEM tab at the bottom of the screen (next page, top left).

And it will open the settings menu (next page, center left).



Here in this section, you can configure various aspects of the emulator. Let's highlight some important details.

In the General section, you can configure various hotkeys and aspects of the emulator related to emulation speed, fast forward, frame-by-frame execution, and access to the DOSBOX.CONF already existing on the machine.

In this menu, you can load the configuration files for a standard DOSBOX installation, which will allow DOSBOX Pure to access your DOS program drive (the folder where you mount your DOS C: drive, if you already have the standard DOSBOX installed), and thus, the execution of your installed programs will be transferred to DOSBOX Pure.

In the INPUT section, you can configure various types of input devices: mouse, joysticks, and keyboards. It is also possible to change the keyboard mapping to a keyboard other than EN-US.


In the Performance section, you can configure the type of machine you want to emulate and access the performance of the emulated machine, with the display of FPS and other information.

In the Video section, you can configure various features for the video emulated in DOSBOX Pure, from the type of video card to the available video memory, and one of the most interesting features of DOSBOX Pure: 3DFx video card emulation.



**3dfx Voodoo emulation**

DOSBOX Pure includes emulation of a 3dfx Voodoo PCI card. Compatible DOS games should work immediately.

There are a few kernel options related to this feature:

**Video > 3dfx Voodoo Emulation**: By default, a compatible 8 MB memory card with a texture mapping unit is emulated. This can be changed to an experimental 12 MB card with two TMUs, a 4 MB card, or the support can be disabled.

**Video > 3dfx Voodoo Performance Settings**: By default, the kernel will use fast OpenGL hardware acceleration to render 3dfx graphics. This setting can be used to switch to software rendering with more faithful emulation, but at a much higher CPU cost.

**Video > 3dfx Voodoo OpenGL Scaling**: Use this setting to increase the OpenGL rendering resolution.

In the Audio section, some precautions must be observed. We will list them below.

**Audio Configuration in DOSBOX Pure**

The audio in DOSBOX Pure can be challenging. Unlike regular DOSBOX, DOSBOX Pure does not emulate an FM sound card with standard MIDI sounds. In fact, you must provide SOUND FONTS for DOSBOX Pure to emulate a sound card.

SOUND FONTS are files in SF2 format and must be placed in the ~/.config/DOSBoxPure/system/ folder.

You can also use the SOUND FONTS from your installed system if you already have sound fonts for MIDI emulation installed.

An interesting website for downloading SOUND FONTS is https://theouterlinux.gitlab.io/Software/Linux/Multimedia/Soundfonts.html

I downloaded two SOUND FONTS and tested each one to see which one would sound best.


However, after some work to get the audio working, I still couldn't get DOSBOX Pure to "sing," so to speak.


**Resolving the lack of sound in DOSBOX Pure**

The silence of DOSBOX Pure was not unique to me. Going to the project's GITHUB, I saw that there was an open ticket from several distros that were unable to get audio with DOSBOX Pure. It should be noted that all non-Debian/ Bunto distros had no sound. Oh, oh... What could be the problem?

It turns out that the author, Bernhard Schelling, made a hard-coded mistake. He instructs DOSBOX Pure to look for an audio library in a location that is only correct on Debian-derived distros, /usr/lib/x86_64- linux-gnu/.

To get sound working on PCLinuxOS, you must do the following:

As root, create the following folder:

```
mkdir /usr/lib/x86_64-linux-gnu
```

Then, create a symbolic link pointing to where the audio library is located:

```
ln -s /usr/lib64/libasound.so.2 /
usr/lib/x64_64-linus-gnu/
libasound.so.2
```

And that's it, your DOSBOX Pure will sing like a nightingale.

The author has acknowledged the error and will correct it in the next version.

**How to install DOSBOX Pure**

I sent the package before writing this article, so I hope it will already be in the PCLinuxOS repositories when the November 2025 issue of PCLOS Magazine comes out. To install, just run apt-get install dosboxpure in a terminal, or through Synaptic or DNF Manager.

Once installed, just click on the icon and the program will open the initial window. Then, drag a folder, a .ZIP file, or an ISO image into the main window and run the game/program.




I hope you enjoy it, as this DOS emulator makes it much easier to run a vast library of DOS programs, with modern features such as 3DFx emulation and resolutions up to 4K.

# Chat Control Is Back On The Menu In The EU. It Still Must Be Stopped

**by Thorin Klosowski**
Electronic Frontier Foundation
Reprinted under Creative Commons license

The European Union Council is once again debating its controversial message scanning proposal, aka "Chat Control," that would lead to the scanning of private conversations of billions of people.

Chat Control, which EFF has strongly opposed since it was first introduced in 2022, keeps being mildly tweaked and pushed by one Council presidency after another.

Chat Control is a dangerous legislative proposal that would make it mandatory for service providers, including end-to-end encrypted communication and storage services, to scan all communications and files to detect "abusive material." This would happen through a method called client-side scanning, which scans for specific content on a device before it's sent. In practice, Chat Control is chat surveillance and functions by having access to everything on a device with indiscriminate monitoring of everything. In a memo, the Danish Presidency claimed this does not break end-to-end encryption.

This is absurd.

We have written extensively that client-side scanning fundamentally undermines end-to-end encryption, and obliterates our right to private spaces. If the government has access to one of the "ends" of an end-to-end encrypted communication, that communication is no longer safe and secure. Pursuing this approach is dangerous for everyone, but is especially perilous for journalists, whistleblowers, activists, lawyers, and human rights workers.

If passed, Chat Control would undermine the privacy promises of end-to-end encrypted communication tools, like Signal and WhatsApp. The proposal is so dangerous that Signal has stated it would pull its app out of the EU if Chat Control is passed. Proponents even seem to realize how dangerous this is, because state communications are exempt from this scanning in the latest compromise proposal.

This doesn't just affect people in the EU, it affects everyone around the world, including in the United States. If platforms decide to stay in the EU, they would be forced to scan the conversation of everyone in the EU. If you're not in the EU, but you chat with someone who is, then your privacy is compromised too. Passing this proposal would pave the way for authoritarian and tyrannical governments around the world to follow suit with their own demands for access to encrypted communication apps.

Even if you take it in good faith that the government would never do anything wrong with this power, events like Salt Typhoon show there's no such thing as a system that's only for the "good guys."

Despite strong opposition, Denmark is pushing forward and taking its current proposal to the Justice and Home Affairs Council meeting on October 14th.

We urge the Danish Presidency to drop its push for scanning our private communication and consider fundamental rights concerns. Any draft that compromises end-to-end encryption and permits scanning of our private communication should be blocked or voted down.

Phones and laptops must work for the users who own them, not act as "bugs in our pockets" in the service of governments, foreign or domestic. The mass scanning of everything on our devices is invasive, untenable, and must be rejected.

# When AI & Secure Chat Meet, Users Deserve Strong Controls Over How They Interact

**by Thorin Klosowski**
Electronic Frontier Foundation


Both Google and Apple are cramming new AI features into their phones and other devices, and neither company has offered clear ways to control which apps those AI systems can access. Recent issues around WhatsApp on both Android and iPhone demonstrate how these interactions can go sideways, risking revealing chat conversations beyond what you intend. Users deserve better controls and clearer documentation around what these AI features can access.

After diving into how Google Gemini and Apple Intelligence (and in some cases Siri) currently work, we didn't always find clear answers to questions about how data is stored, who has access, and what it can be used for.

At a high level, when you compose a message with these tools, the companies can usually see the contents of those messages and receive at least a temporary copy of the text on their servers.

When receiving messages, things get trickier. When you use an AI like Gemini or a feature like Apple Intelligence to summarize or read notifications, we believe companies should be doing that content processing on-device. But poor documentation and weak guardrails create issues that have led us deep into documentation rabbit holes and still fail to clarify the privacy practices as clearly as we'd like.

We'll dig into the specifics below as well as potential solutions we'd like to see Apple, Google, and other device-makers implement, but first things first, here's what you can do right now to control access:

### Control AI Access to Secure Chat on Android and iOS

Here are some steps you can take to control access if you want nothing to do with the device-level AI features' integration and don't want to risk accidentally sharing the text of a message outside of the app you're using.

### How to Check and Limit What Gemini Can Access

If you're using Gemini on your Android phone, it's a good time to review your settings to ensure things are set up how you want. Here's how to check each of the relevant settings:

**Disable Gemini App Activity:** Gemini App Activity is a history Google stores of all your interactions with Gemini. It's enabled by default. To disable it, open Gemini (depending

on your phone model, you may or may not even have the Google Gemini app installed. If you don't have it installed, you don't really need to worry about any of this). Tap your ***profile picture*** > ***Gemini Apps Activity***, then change the toggle to either "Turn off," or "Turn off and delete activity" if you want to delete previous conversations. If the option reads "Turn on," then Gemini Apps Activity is already turned off.

**Control app and notification access:** You can control which apps Gemini can access by tapping your ***profile picture*** > ***Apps***, then scrolling down and disabling the toggle next to any apps you do not want Gemini to access. If you do not want Gemini to potentially access the content that appears in notifications, open the Settings app and revoke notification access from the Google app.

**Delete the Gemini app:** Depending on your phone model, you might be able to delete the Gemini app and revert to using Google Assistant instead. You can do so by long-pressing the Gemini app and selecting the option to delete.

**How to Check and Limit what Apple Intelligence and Siri Can Access**

Similarly, there are a few things you can do to clamp down on what Apple Intelligence and Siri can do:

**Disable the "Use with Siri Requests" option:** If you want to continue using Siri, but don't want to accidentally use it to send messages through secure messaging apps, like WhatsApp, then you can disable that feature by opening ***Settings*** > ***Apps*** > ***[app name]***, and disabling "Use with Siri Requests," which turns off the ability to compose messages with Siri and send them through that app.

**Disable Apple Intelligence entirely:** Apple Intelligence is an all-or-nothing setting on iPhones, so if you want to avoid any potential issues, your only option is to turn it off completely. To do so, open ***Settings*** > ***Apple Intelligence & Siri***, and disable "Apple Intelligence" (you will only see this option if your device supports Apple Intelligence, if it doesn't, the menu will only be for "Siri"). You can also disable certain features, like "writing tools," using Screen Time restrictions. Siri can't be universally turned off in the same way, though you can turn off the options under "Talk to Siri" to make it so you can't speak to it.

For more information about cutting off AI access at different levels in other apps, this Consumer Reports article covers other platforms and services.

**Why It Matters**

**Sending Messages Has Different Privacy Concerns than Receiving Them**

Let's start with a look at how Google and Apple integrate their AI systems into message composition, using WhatsApp as an example.


**Google Gemini and WhatsApp**

On Android, you can optionally link WhatsApp and Gemini together so you can then initiate various actions for sending messages from the Gemini app, like "Call Mom on WhatsApp" or "Text Jason on WhatsApp that we need to cancel our secret meeting, but make it a haiku." This feature raised red flags for users concerned about privacy.

By default, everything you do in Gemini is stored in the "Gemini Apps Activity," where messages are stored forever, subject to human review, and are used to train Google's products. So, unless you change it, when you use Gemini to compose and send a message in WhatsApp, then the message you composed is visible to Google.

If you turn the activity off, interactions are still stored for 72 hours. Google's documentation claims that even though messages are stored, those conversations aren't reviewed or used to improve Google machine learning technologies, though that appears to be an internal policy choice with no technical limits preventing Google from accessing those messages.

The simplicity of invoking Gemini to compose and send a message may lead to a false sense of privacy. Notably, other secure messaging apps, like Signal, do not offer this Gemini integration.

For comparison's sake, let's see how this works with Apple devices.

**Siri and WhatsApp**

The closest comparison to this process on iOS is to use Siri, which it is claimed will eventually be a part of Apple Intelligence. Currently, Apple's AI message composition tools are not available for third-party apps like Signal and WhatsApp.

According to its privacy policy, when you dictate a message through Siri to send to WhatsApp (or anywhere else), the message, including metadata like the recipient phone number and other identifiers, is sent to Apple's servers. This was confirmed by researchers to include the text of messages sent to WhatsApp. When you use Siri to compose a WhatsApp message, the message gets routed to both Apple and WhatsApp. Apple claims it does not store this transcript unless you've opted into "Improve Siri and Dictation." WhatsApp defers to Apple's support for data handling concerns. This is similar to how Google handles speech-to-text prompts.

In response to that research, Apple said this was expected behavior with an app that uses SiriKit — the extension that allows third-party apps to integrate with Siri — like WhatsApp does.

Both Siri and Apple Intelligence can sometimes run locally on-device, and other times need to rely on Apple-managed cloud servers to complete requests. Apple Intelligence can use the company's Private Cloud Compute, but Siri doesn't have a similar feature.

The ambiguity around where data goes makes it overly difficult to decide on whether you are comfortable with the sort of privacy trade-off that using features like Siri or Apple Intelligence might entail.

**How Receiving Messages Works**

Sending encrypted messages is just one half of the privacy puzzle. What happens on the receiving end matters too.

**Google Gemini**

By default, the Gemini app doesn't have access to the text inside secure messaging apps or to notifications. But you can grant access to notifications using the Utilities app. Utilities can read, summarize, and reply to notifications, including in WhatsApp and Signal (it can also read notifications in headphones).

This could open up any notifications routed through the Utilities app to the Gemini app to access internally or from third-parties.

We could not find anything in Google's Utilities documentation that clarifies what information is collected, stored, or sent to Google from these notifications. When we reached out to Google, the company responded that it "builds technical data protections that safeguard user data, uses data responsibly, and provides users with tools to control their Gemini experience." Which means Google has no technical limitation around accessing the text from notifications if you've enabled the feature in the Utilities app.

This could open up any notifications routed through the Utilities app to the Gemini app to be accessed internally or from third-parties. Google needs to publicly make its data handling explicit in its documentation.

If you use encrypted communications apps and have granted access to notifications, then it is worth considering disabling that feature or controlling what's visible in your notifications on an app-level.

**Apple Intelligence**

Apple is more clear about how it handles this sort of notification access.

Siri can read and reply to messages with the "Announce Notifications" feature. With this enabled, Siri can read notifications out loud on select headphones or via CarPlay. In a press release, Apple states, "When a user talks or types to Siri, their request is processed on the device whenever possible. For example, when a user asks Siri to read unread messages… the processing is done on the user's device. The contents of the messages aren't transmitted to Apple servers, because that isn't necessary to fulfill the request."

Apple Intelligence can summarize notifications from any app that you've enabled notifications on. Apple is clear that these summaries are generated on your device, "when Apple Intelligence provides you with preview summaries of your emails, messages, and notifications, these summaries are generated by on-device models." This means there should be

no risk that the text of notifications from apps like WhatsApp or Signal get sent to Apple's servers just to summarize them.

**New AI Features Must Come With Strong User Controls**

As more device-makers cram AI features into their devices, the more necessary it is for us to have clear and simple controls over what personal data these features can access on our devices. If users do not have control over when a text leaves a device for any sort of AI processing—whether that's to a "private" cloud or not—it erodes our privacy and potentially threatens the foundations of end-to-end encrypted communications.

**Per-app AI Permissions**

Google, Apple, and other device makers should add a device-level AI permission, just like they do for other potentially invasive privacy features, like location sharing, to their phones. You should be able to tell the operating system's AI to not access an app, even if that comes at the "cost" of missing out on some features. The setting should be straightforward and easy to understand in ways the Gemini and Apple Intelligence controls currently are not.

**Offer On-Device-Only Modes**

Device-makers should offer an "on-device only" mode for those interested in using some features without having to try to figure out what happens on the device or on the cloud. Samsung offers this, and both Google and Apple would benefit from a similar option.

**Improve Documentation**

Both Google and Apple should improve their documentation about how these features interact with various apps. Apple doesn't seem to clarify notification processing privacy anywhere outside of a press release, and we couldn't find anything about Google's Utilities privacy at all. We appreciate tools like Gemini Apps Activity as a way to audit what the company collects, but vague information like "Prompted a Communications query" is only useful if there's an explanation somewhere about what that means.

The current user options are not enough. It's clear that the AI features device-makers add come with significant confusion about their privacy implications, and it's time to push back and demand better controls. The privacy problems introduced alongside new AI features should be taken seriously, and remedies should be offered to both users and developers who want real, transparent safeguards over how a company accesses their private data and communications.

# An Alternative to Microsoft Office: SoftMaker FreeOffice 2024

**by David Pardue (kalwisti)**

A recent discussion in the PCLinuxOS Forum dealt with the procedure for installing a paid version of the SoftMaker Office suite. I helped the original poster successfully install his downloaded SoftMaker RPM file with a graphical utility, rather than the Terminal/ command line. The last time that I experimented with SoftMaker FreeOffice was many years ago (2012), so I decided this would be a good opportunity to revisit FreeOffice 2024 and see how it has changed.

SoftMaker FreeOffice is a free (of cost) but proprietary office suite developed by SoftMaker Software GmbH in Nuremberg, Germany. The full-featured (paid) version of the program is called SoftMaker Office. (It is a bit confusing because there are actually four versions of SoftMaker Office: two versions of Office NX [subscription-based], and two versions of Office 2024 [Professional and Standard]. Each version has a slightly different feature set, depending on the software's cost. As of June 2025, SM Office 2024 can be purchased from several US-based retailers such as Amazon, B&H, Newegg, Staples and even Walmart.)

Agent Smith (Alessandro) wrote a review of FreeOffice 2021 which was published in the November 2021 issue of our community magazine. Most of the information in the earlier article still applies to FreeOffice 2024, so this refresh will primarily focus on two additional methods of installing the program, as well as providing instructions for uninstalling it.

SoftMaker FreeOffice uses the freemium model, i.e., it has limited functionality compared to the full (paid) version of SoftMaker Office. It is intended to be a demo/introduction to the SM Office suite, and to promote its flagship commercial product. However, for "average" writing tasks, such as composing letters, writing the occasional essay or article, I believe that you will find FreeOffice more than adequate. Another advantage is that FreeOffice 2024 offers these basic features at no cost; once you install (and activate) the software, you may use it for as long as you wish.

Before proceeding, I must mention that installing SM FreeOffice violates one of the standard rules of PCLinuxOS system maintenance: to only install programs from the official PCLinuxOS repository. However, in this case, I can assure you that installing FreeOffice is safe and will not bork your PCLinuxOS installation. I followed the procedure below on two different PCLinuxOS computers and have not experienced any glitches or breakage.

## Download the RPM Package

To get FreeOffice 2024, point your web browser to its Download page, look for the "Linux" box and click on the Download button to download the RPM package.


The RPM file is 99 MB in size.

## Installation Methods

### Command Line

The most efficient way of installing the package is via the command line. Open a Terminal/ Konsole and become the superuser by typing "**$ su -**" *(there is a space and a single hyphen following* **su***)* and entering the root password.

Next, install the RPM file using this command:

```
# rpm -ivh softmaker-freeoffice-2024-1228.x86_64.rpm
```

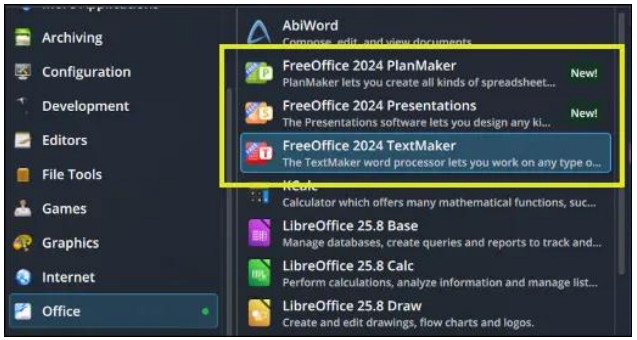
In case you are curious, here is a gloss of the options used in that command:

-i : install
-v : verbose (provide output in the Terminal)
-h : hash (i.e., print 50 hash marks as the package archive is unpacked)

You should see output similar to the following:

```
[root@pclos-darkstar-vb Downloads]# rpm -ivh softmaker-freeoffice-2024-1228.x86_64.rpm
warning: softmaker-freeoffice-2024-1228.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID aa3e7f5e: NOKEY
Verifying...
##################################### [100%]
Preparing...
##################################### [100%]
Updating / installing...
1: softmaker-freeoffice-2024-2024-1228
##################################### [100%]
Extracting resource files...
Using existing xdg-utils
create_script started
Create MIME
Adding document icons. This may take a few minutes...
Updating theme breeze /1 of 2/
Updating theme breeze-dark /1 of 2/
Updating theme hicolor /1 of 2/
Updating theme breeze /2 of 2/
Updating theme breeze-dark /2 of 2/
Updating theme hicolor /2 of 2/
Registering MIME types...
Creating /etc/SoftMaker folder...
Installing for user david
Installing for user root
No default apps file
Cleaning the cache from folder: /var/tmp/kdecache-*/*
Adding icons to the menu...
```

After the package has been installed, entries for the FreeOffice modules will appear in the Office category of your main menu.




(*Note:* If the FreeOffice entries do not appear, log out of your session, then log back in.)

## Graphical RPM Installers

PCLinuxOS has two homegrown graphical installers for locally installing RPM packages: **rpm-installer** and **PkgBuddy** (created by Upgreyed). Although PkgBuddy is a newer utility, I tried both tools and each one worked smoothly.

## PkgBuddy

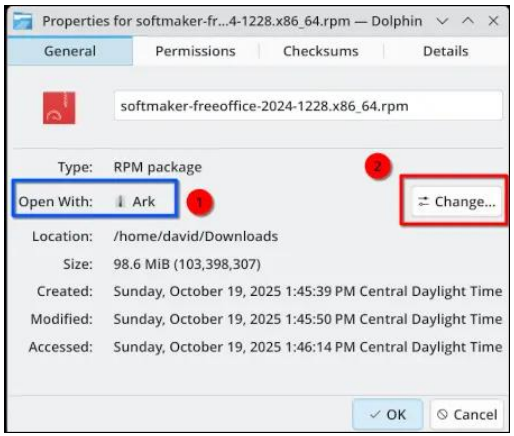
I slightly prefer PkgBuddy because it is a newer tool. You may install the package (name: **pkgbuddy**) via DNF Package Manager or Synaptic. After installing PkgBuddy, follow the steps below to configure it for KDE Plasma 6, MATE or Xfce.

## Configuration in KDE Plasma 6

To use PkgBuddy in KDE 6, follow these steps:

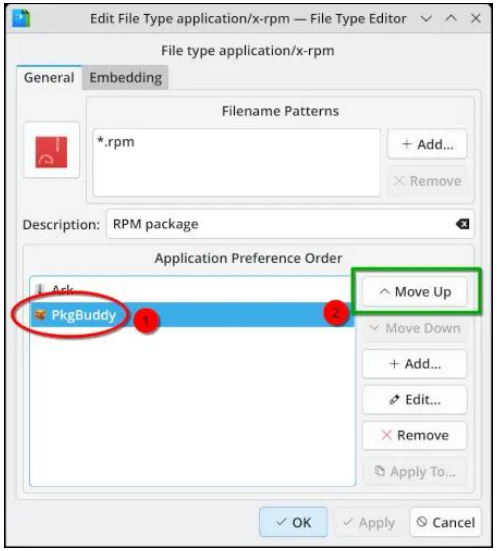
Right-click on the SM FreeOffice RPM file in your **Downloads** folder > and select **Properties**.

Under the **General** tab, look for the **Open With:** line and see if PkgBuddy is listed as the default application.

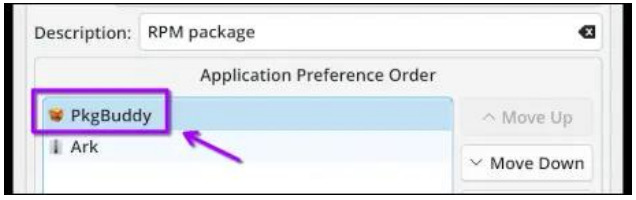


If PkgBuddy happens to be listed as the default, click the OK button to close the dialog box. Then, right-click on the SM FreeOffice RPM file again > and choose **Open with PkgBuddy**.

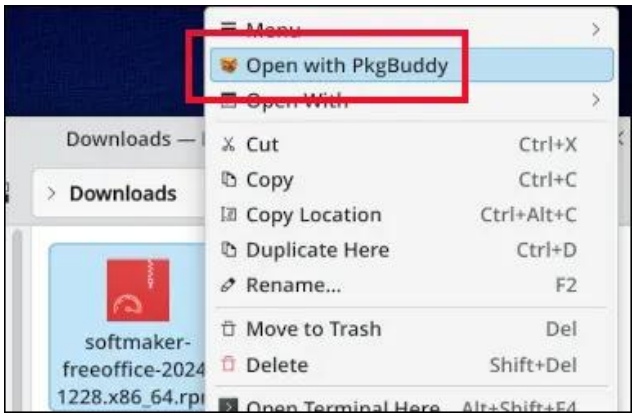
If it is not listed as the default, click on the **Change** button. A dialog box will open, listing the **Application Preference Order:**




Move the entry for PkgBuddy to the top of the list by selecting it and clicking on the **Move Up** button. Then, click the **OK** button in the dialog box to apply the change.

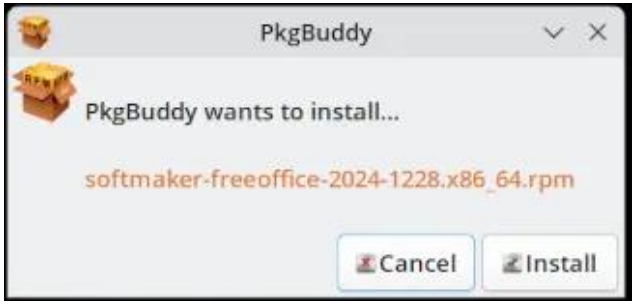



Right-click on the SM FreeOffice RPM file > and choose **Open With PkgBuddy.**




A dialog box will open and prompt you to enter the administrative (root) password.

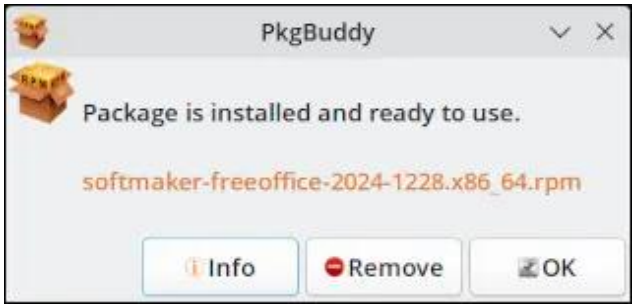

Type the root password and press the **Authenticate** button. A new dialog box will open.




Click on the **Install** button.

*The PkgBuddy dialog box will disappear after a few seconds. Don't panic! The utility is working silently. It will need several minutes to complete the SoftMaker RPM installation.*

A confirmation dialog will appear when the installation finishes.




Click the **OK** button to close the confirmation dialog.

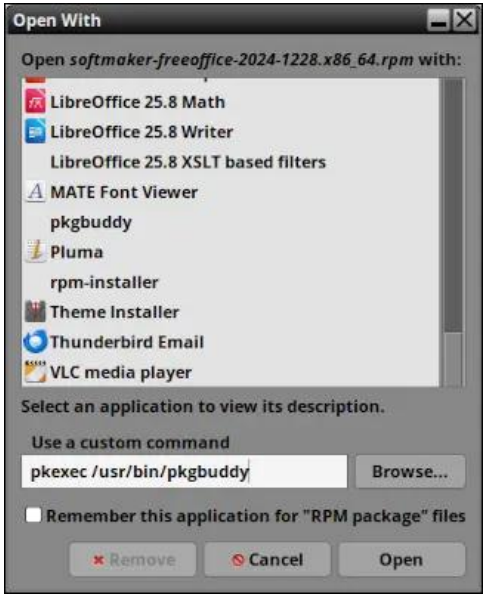
Entries for the FreeOffice modules should appear in the Office category of your main menu. If you do not see those entries, log out of your session, then log back in.

**Configuration in MATE DE**

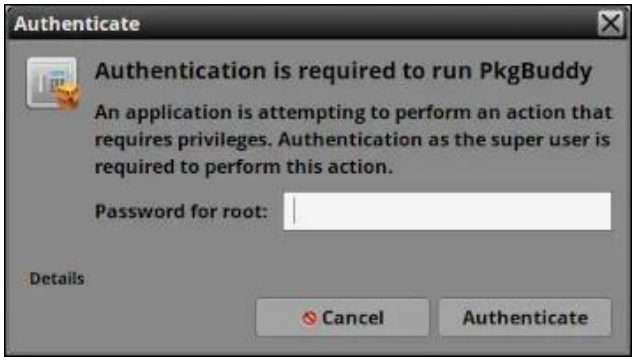
The steps for using PkgBuddy in MATE are very similar to those for KDE Plasma 6.

Right-click on the SM FreeOffice RPM in your **Downloads** folder > and select **Open With Other Application**.

A dialog box will open. Look for the "**Use a custom command**" option and click on it. In the box, type: **pkexec /usr/bin/pkgbuddy**.




Click on the **Open** button. A dialog box will open and prompt you to enter the administrative (root) password.



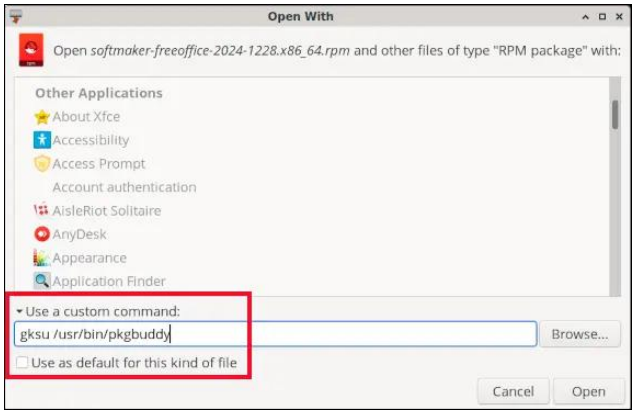

Type the root password to launch PkgBuddy. Afterwards, the remaining steps are identical to those described in the KDE 6 section above.

### Configuration in Xfce

To use PkgBuddy in the Xfce DE, the steps are almost identical to those for MATE above.

Right-click on the SM FreeOffice RPM in your **Downloads** folder > and select **Open With Other Application**.

The main difference is that when you reach the step of "**Use a custom command**", you need to type the command: **gksu /usr/bin/pkgbuddy**.




(*A technical digression*: In a virtual machine with Xfce, I made multiple attempts to get pkexec working properly with the /usr/bin/pkgbuddy command, but was unable to resolve the issue before press time.)

Users have been encouraged to use pkexec as an alternative to the deprecated gksu. In a nutshell, prominent Linux distributions have abandoned the gksu utility due to its security vulnerabilities and unmaintained status, as well as its incompatibility with the Wayland display server.

The recommended replacement for gksu is PolicyKit (pkexec) which is secure and provides granular privilege elevation.

However, gksu is still available in PCLinuxOS. It works, and it should be safe in this situation (*my opinion*) because PkgBuddy has a very limited use case.

### Use of rpm-installer

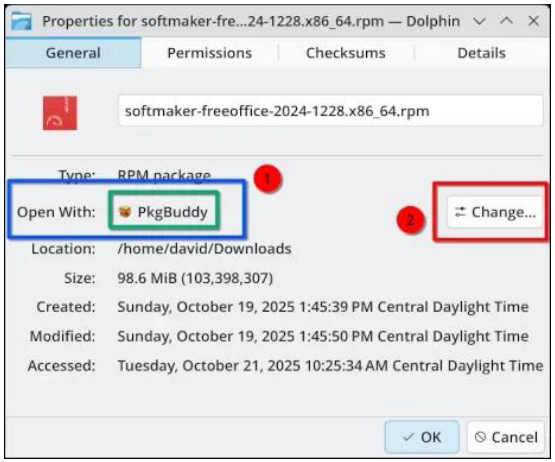
The process of configuring the RPM-Installer utility is very similar to PkgBuddy. Although it is an older tool, it still works reliably. After installing the **rpm-installer** package via DNF Package Manager or Synaptic, follow the steps below.

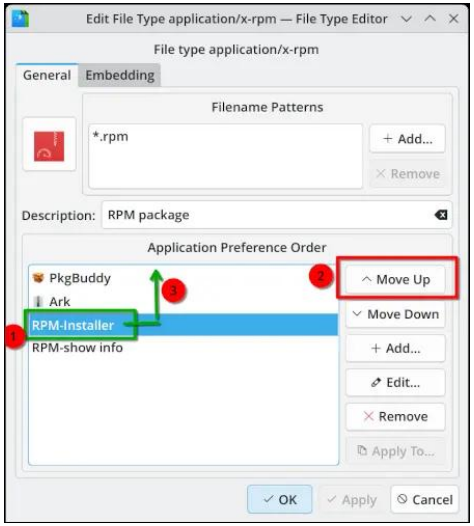
### In KDE Plasma 6

Right-click on the SM FreeOffice RPM in your **Downloads** folder > and select **Properties**.

Under the **General** tab, look for the **Open With**: line. If RPM-Installer is not the default choice, click on the **Change** button (next page, top left).

A dialog box will open, displaying the **Application Preference Order**. Move the entry for RPM-Installer to the top of the list by selecting it and clicking on the **Move Up** button. Then, click the **OK** button to apply the change (next page, left center).

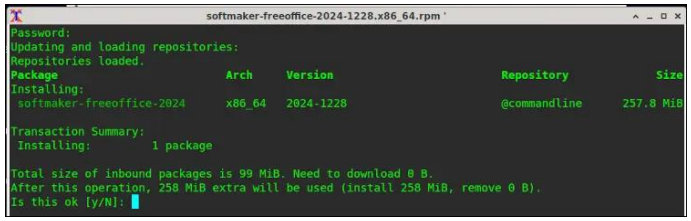


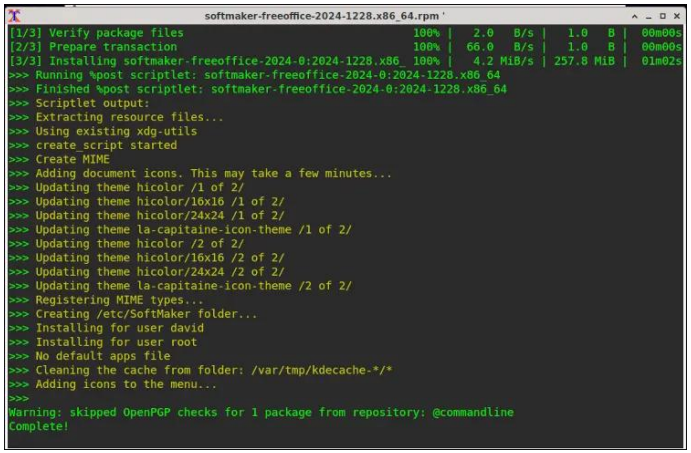

Next, right-click again on the SM FreeOffice RPM icon > and choose **Open with RPM-Installer**.

This will launch an Xterm terminal emulator window. You will be prompted to enter the root password.

Type "**y**" to proceed with installing the software.




Wait patiently while the installation takes place. You should see Xterm output similar to the screenshot below.



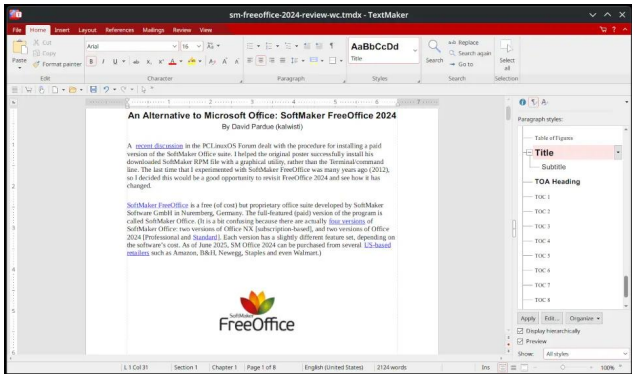

After RPM-Installer finishes, close the Xterm window by clicking on the Close (X) button.

Entries for the FreeOffice modules will appear in the Office category of your main menu. If you do not see those entries, log out of your session, then log back in.

## My Impressions

Word processing is my main activity, so I concentrated on evaluating TextMaker. It is pleasant to use; I wrote this article with it, using FreeOffice's native .tmdx file format, then saved the file in ODF (Open Document Format, viz. .odt) and made final layout adjustments with LibreOffice Writer before submitting it to the magazine.

For me, the most crucial missing features are the lack of footnotes/endnotes, no capability for generating a table of contents and the inability to navigate within the document via the Sidebar. Some other limitations which do not bother me, but might be important to your workflow, include: no capability for adding comments or tracking changes; no index generation; no grammar check or thesaurus.




PlanMaker, the spreadsheet module, can open .ods files but cannot Save As in ODF format. The "**Save As**" options are .pmdx (SM-native format), .xlsx, .xls, .csv, .html and .txt. PlanMaker is not able to execute macros and VBA scripts stored in MS Excel documents.

The Presentations module cannot open Open Document .odp files at all. The "Save As" options are: .prdx (SM-native format), .pptx, and .ppt.

On the positive side, I experimented with opening a variety of MS Office-generated files, such as document templates from Microsoft's Create gallery as well as spreadsheets from data.gov. FreeOffice 2024 did a good job of faithfully reproducing the Office-formatted documents.

Registering FreeOffice 2024 after its 10-day trial period was straightforward; I just provided my e-mail address. (The submission form did not ask for my name.) I received an Activation number via e-mail, then entered it by clicking on the "?" icon (*top right corner of the toolbar*) > and selecting "**Manage license …**".

The terms of FreeOffice's license are reasonable, in my opinion. The license allows FreeOffice to be used on 3 computers that belong to the same family household — on any combination of Linux, macOS, and MS Windows — or on 1 computer that belongs to an organization.

**Removing / Uninstalling FreeOffice 2024**

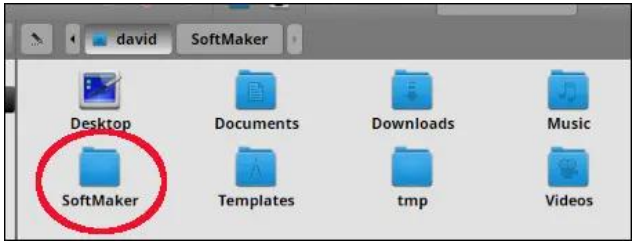
If you change your mind and wish to uninstall FreeOffice 2024, you must use the Terminal/ Konsole. First, become the superuser by typing "**$ su -**" (*there is a space and a single hyphen following* **su**) and entering the root password.

Either one of the commands below will remove the program:

```
# rpm -e softmaker-freeoffice-2024-2024-1228
```

```
# dnf remove softmaker-freeoffice-2024.x86_64
```

After the system-level files have been deleted, you will need to manually delete the **SoftMaker** directory that was created within your **/home** directory. You may use your DE's file manager (Dolphin, Thunar, Caja, etc.) to accomplish this.




**Summary**

SoftMaker FreeOffice 2024 is a worthwhile option if you need an office suite that is free, cross-platform and more lightweight than LibreOffice. FreeOffice features high compatibility with Microsoft Office files, and its interface resembles MS Office (if you choose the "ribbon" design). TextMaker is a more powerful word processor than AbiWord. Since SM Office is made in the European Union, it is GDPR (General Data Protection Regulation)-compliant. The GDPR ensures the privacy and protection of personal information.

I will not criticize SoftMaker for limiting features on FreeOffice; from a business perspective, SoftMaker cannot survive without revenue. Software costs money — especially in a changing environment where the software needs to be constantly developed.

Martin Kotulla, the founder and CEO of SoftMaker, pointed out in an interview that SoftMaker is a relatively small company with 65 employees: 25 full-time staff in their Nuremberg headquarters, and around 40 freelancers in Germany and elsewhere around the world. When compared with their main competitors — Microsoft and Google — who have nearly unlimited funds and thousands of employees, it is a David vs. Goliath scenario.

If you are considering the full (paid) version of SoftMaker Office, keep an eye open for their frequent sales/discount offers.

**Additional Resources**

User manuals for TextMaker, PlanMaker and Presentations are available here:

Download: Free manuals for FreeOffice

There is an English-language Support forum:

SoftMaker.com Support Forum (English)

The FreeOffice 2024 for Linux section can be accessed at:

SoftMaker.com - FreeOffice 2024 for Linux

If you can read German, there is also a German-language Support forum:

SoftMaker Support Forum (German)

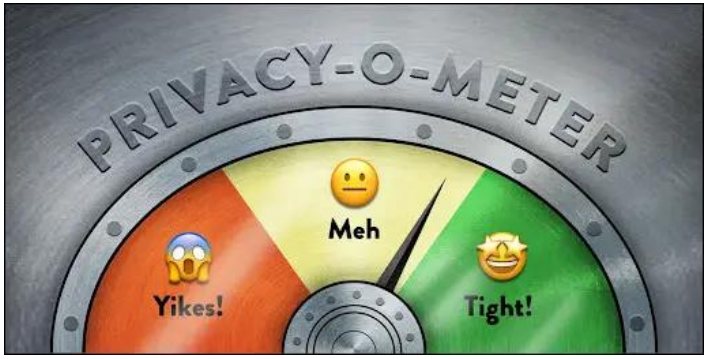
# Daily Tips to Protect Your Privacy and Security

**by Thorin Klosowski, Lena Cohen, Christian Romero, Hayley Tsukayama, Bill Budington, Rindala Alajaji, Yael Grauer, and Paige Collings**
Electronic Frontier Foundation


Trying to take control of your online privacy can feel like a full-time job. But if you break it up into small tasks and take on one project at a time, it makes the process of protecting your privacy much easier. This month we're going to do just that. For the month of October, we'll update this post with new tips every weekday that show various ways you can opt yourself out of the ways tech giants surveil you.

Online privacy isn't dead. But the tech giants make it a pain in the butt to achieve. With these incremental tweaks to the services we use, we can throw sand in the gears of the surveillance machine and opt out of the ways tech companies attempt to optimize us into advertisement and content viewing machines. We're also pushing companies to make more privacy-protective defaults the norm, but until that happens, the onus is on all of us to dig into the settings.

*All month long we'll share tips, including some with the help from our friends at Consumer Reports' Security Planner tool.*




**Tip 1: Establish Good Digital Hygiene**

Before we can get into the privacy weeds, we need to first establish strong basics. Namely, two security fundamentals: using strong passwords (a password manager helps simplify this) and two-factor authentication for your online accounts. Together, they can significantly improve your online privacy by making it much harder for your data to fall into the hands of a stranger.

Using unique passwords for every web login means that if your account information ends up in a data breach, it won't give bad actors an easy way to unlock your *other* accounts. Since it's impossible for all of us to remember a unique password for every login we have, most people will want to use a password manager, which generates and stores those passwords for you.

Two-factor authentication is the second lock on those same accounts. In order to login to, say, Facebook for the first time on a particular computer, you'll need to provide a password and a "second factor," usually an always-changing numeric code generated in an app or sent to you on another device. This makes it much harder for someone else to get into your account because it's less likely they'll have both a password and the temporary code.

This can be a little overwhelming to get started if you're new to online privacy! Aside from our guides on Surveillance Self-Defense, we recommend taking a look at Consumer Reports' Security Planner for ways to help you get started setting up your first password manager and turning on two-factor authentication.

**Tip 2: Learn What a Data Broker Knows About You**

Hundreds of data brokers you've never heard of are harvesting and selling your personal information. This can include your address, online activity, financial transactions, relationships, and even your location history. Once sold, your data can be abused by scammers, advertisers, predatory companies, and even law enforcement agencies.

Data brokers build detailed profiles of our lives but try to keep their own practices hidden. Fortunately, several state privacy laws give you the right to see what information these

companies have collected about you. You can exercise this right by submitting a data access request to a data broker. Even if you live in a state without privacy legislation, some data brokers will still respond to your request.

There are hundreds of known data brokers, but here are a few major ones to start with:

- Acxiom
- Epsilon
- The Trade Desk

Data brokers have been caught ignoring privacy laws, so there's a chance you won't get a response. If you do, you'll learn what information the data broker has collected about you and the categories of third parties they've sold it to. If the results motivate you to take more privacy action, encourage your friends and family to do the same. Don't let data brokers keep their spying a secret.

You can also ask data brokers to delete your data, with or without an access request. We'll get to that later this month and explain how to do this with people-search sites, a category of data brokers.

**Tip 3: Disable Ad Tracking on iPhone and Android**

Picture this: you're doomscrolling and spot a t-shirt you love. Later, you mention it to a friend and suddenly see an ad for that exact shirt in another app. The natural question pops into your head: *"Is my phone listening to me?"* Take a sigh of relief because, no, your phone is not listening to you. But advertisers are using shady tactics to profile your interests. Here's an easy way to fight back: disable the ad identifier on your phone to make it harder for advertisers and data brokers to track you.

**Disable Ad Tracking on iOS and iPadOS:**

- Open *Settings* > *Privacy & Security* > *Tracking*, and turn off "Allow Apps to Request to Track."
- Open *Settings* > *Privacy & Security* > *Apple Advertising*, and disable "Personalized Ads" to also stop some of Apple's internal tracking for apps like the App Store.
- If you use Safari, go to *Settings* > *Apps* > *Safari* > *Advanced* and disable "Privacy Preserving Ad Measurement."

**Disable Ad Tracking on Android:**

- Open *Settings* > *Security & privacy* > *Privacy controls* > *Ads*, and tap "Delete advertising ID"
- While you're at it, run through Google's "Privacy Checkup" to review what info other Google services—like YouTube or your location—may be sharing with advertisers and data brokers.

These quick settings changes can help keep bad actors from spying on you. For a deeper dive on securing your iPhone or Android device, be sure to check out our full Surveillance Self-Defense guides.

**Tip 4: Declutter Your Apps**

Decluttering is all the rage for optimizers and organizers alike, but did you know a cleansing sweep through your apps can also help your privacy? Apps collect a lot of data, often in the background when you are not using them. This can be a prime way companies harvest your information, and then repackage and sell it to *other* companies you've never heard of. Having a lot of apps increases the peepholes that companies can gain into your personal life.

Do you need *three* airline apps when you're not even traveling? Or the app for that hotel chain you stayed in once? It's best to delete that app and cut off their access to your information. In an ideal world, app makers would not process any of your data unless strictly necessary to give you what you asked for. Until then, to do an app audit:

- Look through the apps you have and identify ones you rarely open or barely use.
- Long-press on apps that you don't use anymore, and delete or uninstall them when a menu pops up.
- Even on apps you keep, take a swing through the location, microphone, or camera

permissions for each of them. For iOS devices, you can follow these instructions to find that menu. For Android, check out this instructions page.

If you delete an app and later find you need it, you can always redownload it. Try giving some apps the boot today to gain some memory space and some peace of mind.

**Tip 5: Disable Behavioral Ads on Amazon**

Happy Amazon Prime Day! Let's celebrate by taking back a piece of our privacy.

Amazon collects an astounding amount of information about your shopping habits. While the only way to truly free yourself from the company's all-seeing eye is to never shop there, there is something you can do to disrupt *some* of that data use: tell Amazon to stop using your data to market more things to you (these settings are for US users and may not be available in all countries).

- Log into your Amazon account, then click "Account & Lists" under your name.
- Scroll down to the "Communication and Content" section and click "Advertising preferences" (or just click this link to head directly there).
- Click the option next to "Do not show me interest-based ads provided by Amazon."
- You may want to also delete the data Amazon already collected, so click the "Delete ad data" button.

This setting will turn off the personalized ads based on what Amazon infers about you, though you will likely still see recommendations based on your past purchases at Amazon.

Of course, Amazon sells a lot of other products. If you own an Alexa, now's a good time to review the few remaining privacy options available to you after the company took away the ability to disable voice recordings. Kindle users might want to turn off some of the data usage tracking. And if you own a Ring camera, consider enabling end-to-end encryption to ensure you're in control of the recording, not the company.

**Tip 6: Install Privacy Badger to Block Online Trackers**

Every time you browse the web, you're being tracked. Most websites contain invisible tracking code that lets companies collect and profit from your data. That data can end up in the hands of advertisers, data brokers, scammers, and even government agencies. Privacy Badger, EFF's free browser extension, can help you fight back.

Privacy Badger automatically blocks hidden trackers to stop companies from spying on you online. It also tells websites not to share or sell your data by sending the "Global Privacy Control" signal, which is legally binding under some state privacy laws. Privacy Badger has evolved over the past decade to fight various methods of online tracking. Whether you want to protect your sensitive information from data brokers or just don't want Big Tech monetizing your data, Privacy Badger has your back.

**Visit privacybadger.org to install Privacy Badger.**

It's available on Chrome, Firefox, Edge, and Opera for desktop devices and Firefox and Edge for Android devices. Once installed, all of Privacy Badger's features work automatically. There's no setup required! If blocking harmful trackers ends up breaking something on a website, you can easily turn off Privacy Badger for that site while maintaining privacy protections everywhere else.

When you install Privacy Badger, you're not just protecting yourself—you're joining EFF and millions of other users in the fight against online surveillance.

**Tip 7: Review Location Tracking Settings**

Data brokers don't just collect information on your purchases and browsing history. Mobile apps that have the location permission turned on will deliver your coordinates to third parties in exchange for insights or monetary kickbacks. Even when they don't deliver that data directly to data brokers, if the app serves ad space, your location will be delivered in real-time bid requests not only to those wishing to place an ad, but to all participants in the ad auction—

even if they lose the bid. Location data brokers take part in these auctions just to harvest location data en masse, without any intention of buying ad space.

Luckily, you can change a few settings to protect yourself against this hoovering of your whereabouts. You can use iOS or Android tools to audit an app's permissions, providing clarity on who is providing what info to whom. You can then go to the apps that don't need your location data and disable their access to that data (you can always change your mind later if it turns out location access was useful). You can also disable real-time location tracking by putting your phone into airplane mode, while still being able to navigate using offline maps. And by disabling mobile advertising identifiers (see tip Three), you break the chain that links your location from one moment to the next.

Finally, for particularly sensitive situations you may want to bring an entirely separate, single-purpose device which you've kept clean of unneeded apps and locked down settings on. Similar in concept to a burner phone, even if this single-purpose device does manage to gather data on you, it can only tell a partial story about you—all the other data linking you to your normal activities will be kept separate.

For details on how you can follow these tips and more on your own devices, check out our more extensive post on the topic.


**Tip 8: Limit the Data Your Gaming Console Collects About You**

Oh, the beauty of gaming consoles—just plug in and play! Well... after you speed-run through a bunch of terms and conditions, internet setup, and privacy settings. If you rushed through those startup screens, don't worry! It's not too late to limit the data your console is collecting about you. Because yes, modern consoles do collect a lot about your gaming habits.

Start with the basics: make sure you have two-factor authentication turned on for your accounts. PlayStation, Xbox, and Nintendo all have guides on their sites. Between payment details and other personal info tied to these accounts, 2FA is an easy first line of defense for your data.

Then, it's time to check the privacy controls on your console:

- **PlayStation 5**: Go to ***Settings*** > ***Users and Accounts*** > ***Privacy*** to adjust what you share with both strangers and friends. To limit the data your PS5 collects about you, go to ***Settings*** > ***Users and Accounts*** > ***Privacy***, where you can adjust settings under ***Data You Provide*** and ***Personalization***.

- **Xbox Series X|S**: Press the ***Xbox button*** > ***Profile & System*** > ***Settings*** > ***Account*** > ***Privacy & online safety*** > ***Xbox Privacy*** to fine-tune your sharing. To manage data collection, head to ***Profile & System*** > ***Settings*** > ***Account*** > ***Privacy & online safety*** > ***Data collection***.

- **Nintendo Switch**: The Switch doesn't share as much data by default, but you still have options. To control who sees your play activity, go to ***System Settings*** > ***Users*** > ***[your profile]*** > ***Play Activity Settings***. To opt out of sharing eShop data, open the eShop, select your profile (top right), then go to ***Google Analytics Preferences*** > ***Do Not Share***.

Plug and play, right? Almost. These quick checks can help keep your gaming sessions fun —and more private.

**Tip 9: Hide Your Start and End Points on Strava**

Sharing your personal fitness goals, whether it be extended distances, accurate calorie counts, or GPS paths—sounds like a fun, competitive feature offered by today's digital fitness trackers. If you enjoy tracking those activities, you've probably heard of Strava. While it's excellent for motivation and connecting with fellow athletes, Strava's default settings can reveal sensitive information about where you live, work, or exercise, creating serious security and privacy risks. Fortunately, Strava gives you control over how much of your activity map is visible to others, allowing you to stay active in your community while protecting your personal safety.

We've covered how Strava data exposed classified military bases in 2018 when service members used fitness trackers. If fitness data can compromise national security, what's it revealing about you?

Here's how to hide your start and end points:

- **On the website**: Hover over your profile picture > ***Settings > Privacy Controls > Map Visibility.***

- **On mobile**: Open ***Settings > Privacy Controls > Map Visibility.***

- You can then choose from three options: hide portions near a specific address, hide start/end of all activities, or hide entire maps.

You can also adjust individual activities:

- Open the activity you want to edit.

- Select the three-dot menu icon.

- Choose “Edit Map Visibility.”

- Use sliders to customize what's hidden or enable “Hide the Entire Map.”

Great job taking control of your location privacy! Remember that these settings only apply to Strava, so if you share activities to other platforms, you'll need to adjust those privacy settings separately. While you're at it, consider reviewing your overall activity visibility settings to ensure you're only sharing what you want with the people you choose.

**Tip 10: Find and Delete An Account You No Longer Use**

Millions of online accounts are compromised each year. The more accounts you have, the more at risk you are of having your personal data illegally accessed and published online. Even if you don’t suffer a data breach, there’s also the possibility that someone could find one of your abandoned social media accounts containing information you shared publicly on purpose in the past, but don’t necessarily want floating around anymore. And companies may still be profiting off details of your personal life, even though you’re not getting any benefit from their service.

So, now’s a good time to find an old account to delete. There may be one you can already think of, but if you’re stuck, you can look through your password manager, look through logins saved on your web browser, or search your email inbox for phrases like “new account,” “password,” “welcome to,” or “confirm your email.” Or, enter your email address on the website HaveIBeenPwned to get a list of sites where your personal information has been compromised to see if any of them are accounts you no longer use.

Once you’ve decided on an account, you’ll need to find the steps to delete it. Simply deleting an app off of your phone or computer does not delete your account. Often you can log in and look in the account settings, or find instructions in the help menu, the FAQ page, or the pop-up customer service chat. If that fails, use a search engine to see if anybody else has written up the steps to deleting your specific type of account.

For more information, check out the Delete Unused Accounts tip on Security Planner.

**Tip 11: Search for Yourself**

Today's tip may sound a little existential, but we're not suggesting a deep spiritual journey. Just a trip to your nearest search engine. Pop your name into search engines such as Google or DuckDuckGo, or even AI tools such as ChatGPT, to see what you find. This is one of the simplest things you can do to raise your own awareness of your digital reputation. It can be the first thing prospective employers (or future first dates) do when trying to figure out who you are. From a privacy perspective, doing it yourself can also shed light on how your information is presented to the general public. If there's a defunct social media account you'd rather keep hidden, but it's on the first page of your search results, that might be a good signal for you to finally delete that account. If you shared your cellphone number with an organization you volunteer for, and it's on their home page, you can ask them to take it down.

Knowledge is power. It's important to know what search results are out there about you, so you understand what people see when they look for you. Once you have this overview, you can make better choices about your online privacy.

**Tip 12: Tell “People Search” Sites to Delete Your Information**

When you search online for someone’s name, you’ll likely see results from people-search sites selling their home address, phone number, relatives’ names, and more. People-search sites are a type of data broker with an especially

dangerous impact. They can expose people to scams, stalking, and identity theft. Submit opt out requests to these sites to reduce the amount of personal information that is easily available about you online.

Check out this list of opt-out links and instructions for more than 50 people search sites, organized by priority. Before submitting a request, check that the site actually has your information. Here are a few high-priority sites to start with:

- **Intelius**: Find your information and fill out the opt-out form.
- **Spokeo**: Find your information and enter the URL of your profile on the opt-out page.
- **BeenVerified**: Find your information and opt out of people search and property search.

Data brokers continuously collect new information, so your data could reappear after being deleted. You'll have to re-submit opt-outs periodically to keep your information off of people-search sites. Subscription-based services can automate this process and save you time, but a Consumer Reports study found that manual opt-outs are more effective.

**Tip 13: Remove Your Personal Addresses from Search Engines**

Your home address may often be found with just a few clicks online. Whether you're concerned about your digital footprint or looking to safeguard your physical privacy, understanding where your address appears and how to remove or obscure it is a crucial step. Here's what you need to know.

Your personal addresses can be available through public records like property purchases, medical licensing information, or data brokers. Opting out from data brokers will do a lot to remove what's available commercially, but sometimes you can't erase the information entirely from things like property sales records.

You can ask some search engines to remove your personal information from search indexes, which is the most efficient way to make information like your personal addresses, phone number, and email address a lot harder to find. Google has a form that makes this request quite easy, and we'd suggest starting there.

**Day 14: Check Out Signal**

Here's the problem: many of your texts aren't actually private. Phone companies, government agencies, and app developers all too often can all peek at your conversations.

So on Global Encryption Day, our tip is to check out Signal—a messaging app that actually keeps your conversations private.

Signal uses end-to-end encryption, meaning only you and your recipient can read your messages—not even Signal can see them. Security experts love Signal because it's run by a privacy-focused nonprofit, funded by donations instead of data collection, and its code is publicly auditable.

Beyond privacy, Signal offers free messaging and calls over Wi-Fi, helping you avoid SMS charges and international calling fees. The only catch? Your contacts need Signal too, so start recruiting your friends and family!

**How to get started**: Download Signal from your app store, verify your phone number, set a secure PIN, and start messaging your contacts who join you. Consider also setting up a username, so people can reach you without sharing your phone number. For more detailed instructions, check out our guide.

Global Encryption Day is the perfect timing to protect your communications. Take your time to explore the app, and check out other privacy protecting features like disappearing messages, session verification, and lock screen notification privacy.

**Tip 15: Switch to a Privacy-Protective Browser**

Your browser stores tons of personal information: browsing history, tracking cookies, and data that companies use to build detailed profiles for targeted advertising. The browser you choose makes a huge difference in how much of this tracking you can prevent.

Most people use Chrome or Safari, which are automatically installed on Google and Apple products, but these browsers have significant

privacy drawbacks. For example: Chrome's Incognito mode only hides history on your device—it doesn't stop tracking. Safari has been caught storing deleted browser history and collecting data even in private browsing mode.

Firefox is one alternative that puts privacy first. Unlike Chrome, Firefox automatically blocks trackers and ads in Private Browsing mode and prevents websites from sharing your data between sites. It also warns you when websites try to extract your personal information. But Firefox isn't your only option—other privacy-focused browsers like DuckDuckGo, Brave, and Tor also offer strong protections with different features. The key is switching away from browsers that prioritize data collection over your privacy.

Switching is easy: download your chosen browser from the links above and install it. Most browsers let you import bookmarks and passwords during setup.

You now have a new browser! Take some time to explore your new browser's privacy settings to maximize your protection.

**Tip 16: Give Yourself Another Online Identity**

We all take on different identities at times. Just as it's important to set boundaries in your daily life, the same can be true for your digital identity. For many reasons, people may want to keep aspects of their lives separate—and giving people control over how their information is used is one of the fundamental reasons we fight for privacy. Consider chopping up pieces of your life over separate email accounts, phone numbers, or social media accounts.

This can help you manage your life and keep a full picture of your private information out of the hands of nosy data-mining companies. Maybe you volunteer for an organization in your spare time that you'd rather keep private, want to keep emails from your kids' school separate from a mountain of spam, or simply would rather keep your professional and private social media accounts separate.

Whatever the reason, consider whether there's a piece of your life that could benefit from its own identity. When you set up these boundaries, you can also protect your privacy.

**Tip 17: Check Out Virtual Card Services**

Ever encounter an online vendor selling something that's just what you need—if you could only be sure they aren't skimming your credit card number? Or maybe you trust the vendor, but aren't sure the website (seemingly written in some arcane e-commerce platform from 1998) won't be hacked within the hour after your purchase? Buying those bits and bobs shouldn't cost you your peace of mind on top of the dollar amount. For these types of purchases, we recommend checking out a virtual card service.

These services will generate a seemingly random credit card for your use which is locked down in a particular way which you can specify. This may mean a card locked to a single vendor, where no one else can make charges on it. It could only validate charges for a specific category of purchase, for example, clothing. You can not only set limits on vendors, but set spending limits a card can't exceed, or that it should just be a one-time use card and then close itself. You can even pause a card if you are sure you won't be using it for some time, and then unpause it later. The configuration is up to you.

There are a number of virtual card services available, like Privacy.com or IronVest, just to name a few. Just like any vendor, though, these services need some way to charge you. So for any virtual card service, pop them into your favored search engine to verify they're legit, and aren't going to burden you with additional fees. Some options may also only be available in specific countries or regions, due to financial regulation laws.


# GIMP Tutorial: Create A Gold Paint Effect

**by Meemaw**

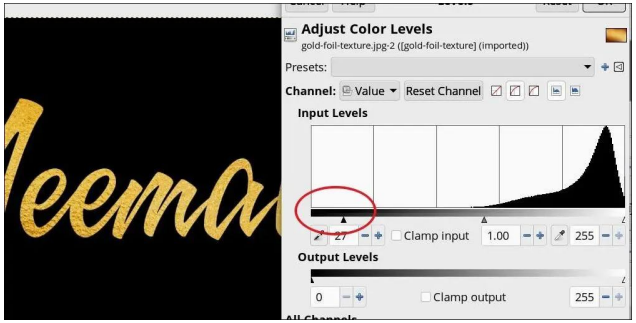
I sometimes look on YouTube to find ideas about tutorials that I think are useful. One area I look for is text effects. When you're doing a design, it helps to be able to configure any text you have in different ways. Logos by Nick did this one about six years ago, but it's a good one. It's a Gold Foil effect.

There are several places you can find a gold foil texture to use. Nick even provided one in his tutorial. I got one from Pixabay.

Start by loading your gold foil texture. Add a layer above, filled with black. Now add white text, using a brush or script style. I did this several times, using Great Vibes and A&S Speedway fonts.

In the layers dialog, select the text layer, right-click and choose **Alpha to selection**. Now, delete the text layer using the tool in the layers dialog. On the black layer, press the delete key to let the gold show through. Now choose **Select > None** to clear your selection and proceed.

Click on the gold layer and then choose **Color > Levels**. Adjust levels, so the gold has more varied colors. How far you move the slider depends on how varied you want your colors and how light or dark your background is.

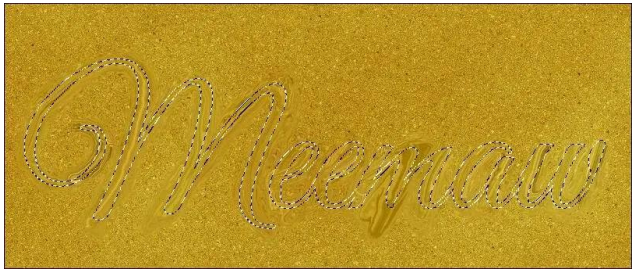



We're going to use the **Warp transform** tool. Set it to **Move Pixels**. Choose a hard brush. **Tool Settings** should be:

**Brush size** — about 70 depending on font size, but it could be less.
**Hardness** — about 75
**Strength** — about 80
**Spacing** — about 50

Paint with the brush to make the gold look more streaked, like the text was written (one gold leaf pattern looks kinda bubbly, and the other looks kinda glittery). Painting with the Warp Transform tool is a bit fiddly, and it's your choice how much you want to do.

Using the black layer, choose **Alpha to selection**. GIMP will choose the text. Delete the black layer. Now you'll have what looks kinda messy with the text selected.



Add an Alpha channel to the gold layer, then press **Delete**. You will get gold text on a transparent background.

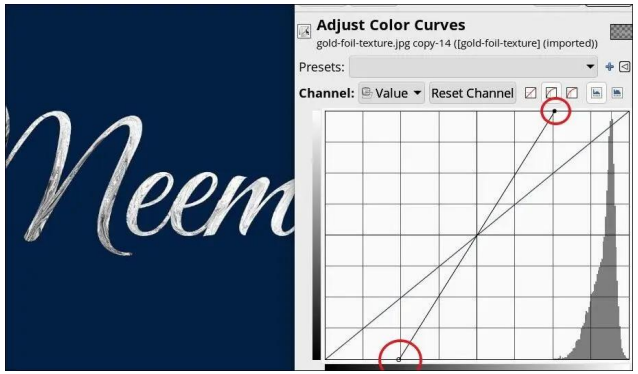
Choose **Select > None** again.

You can add another layer with the background you want (next page, top left).

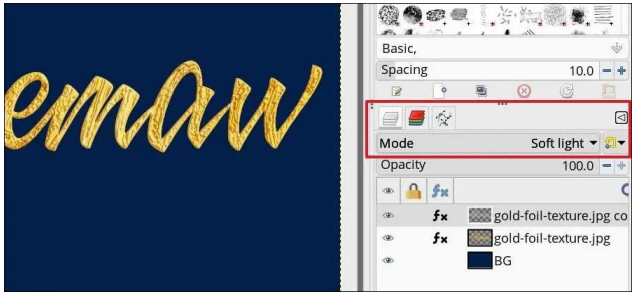
We could stop here, if you're happy with what you have. You can also do another step to give it a sort of oil paint texture. Duplicate the gold


layer & select the new layer. Remove the saturation by choosing **Colors** > **Saturation** and move the slider left to 0.

Now choose **Colors** > **Curves** and move each end toward the other side along the window edges. This brings more dark out (moving the bottom left curve) and more white (moving the upper right curve). How far you go is up to you.

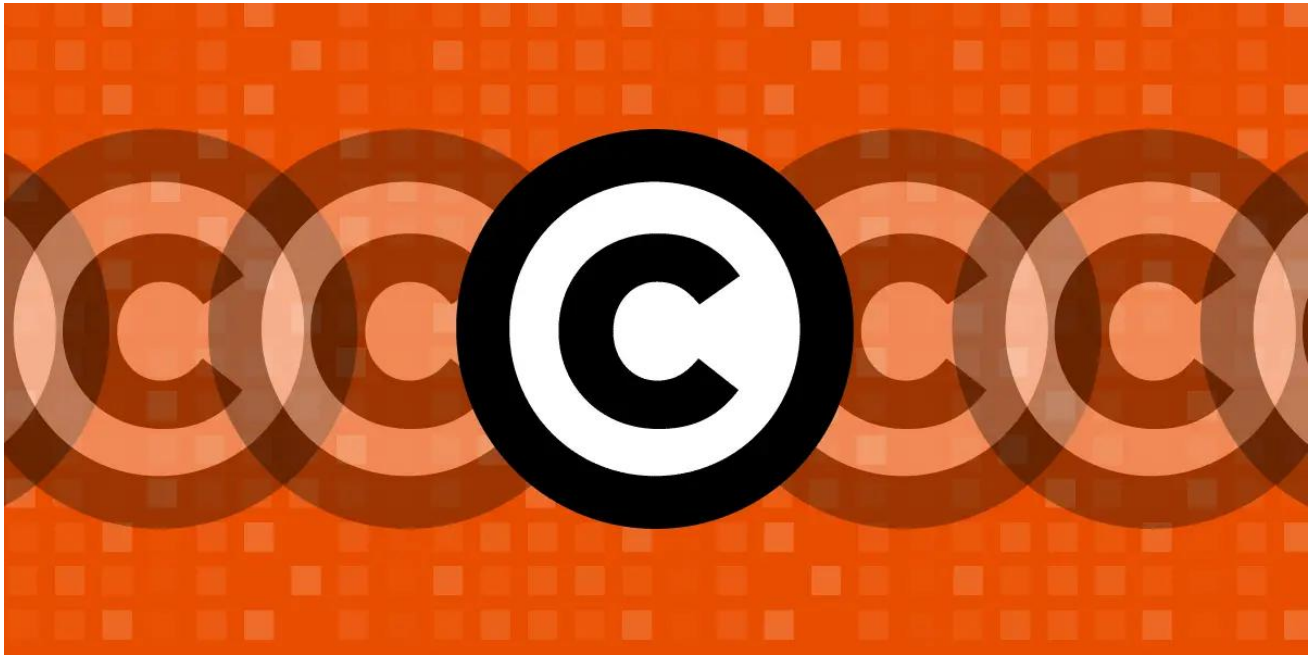



Add a slight Gaussian blur, choosing **Filters** > **Blur** > **Gaussian Blur**. Set it to 1.0. Now choose **Filters** > **Distorts** > **Emboss**. Keep the defaults and click OK. Go to the Layers dialog, and change the blend mode to **Soft Light** (center, top).




The last one I did ended up having a purple background.

# Protecting Access To The Law — And Beneficial Uses Of AI



**by Mitch Stoltz**
Electronic Frontier Foundation


As the first copyright cases concerning AI reach appeals courts, EFF wants to protect important, beneficial uses of this technology—including AI for legal research. That's why we weighed in on the long-running case of Thomson Reuters v. ROSS Intelligence. This case raises at least two important issues: the use of (possibly) copyrighted material to train a machine learning AI system, and public access to legal texts.

ROSS Intelligence was a legal research startup that built an AI-based tool for locating judges' written opinions based on natural language queries—a competitor to ubiquitous legal research platforms like Lexis and Thomson Reuters' Westlaw. To build its tool, ROSS hired another firm to read through thousands of the "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. ROSS used those paraphrases to train its tool. Importantly, the ROSS tool didn't output any West headnotes, or even the paraphrases of those headnotes—it simply directed the user to the original judges' decisions. Still, Thomson sued ROSS for copyright infringement, arguing that using the headnotes without permission was illegal.

Early decisions in the suit were encouraging. EFF wrote about how the court allowed ROSS to bring an antitrust counterclaim against Thomson Reuters, letting them try to prove that Thomson was abusing monopoly power. And the trial judge initially ruled that ROSS's use of the West headnotes was fair use under copyright law.

The case then took turns for the worse. ROSS was unable to prove its antitrust claim. The trial judge issued a new opinion, reversing his earlier decision and finding that ROSS's use was not fair but rather infringed Thomson's copyrights. And in the meantime, ROSS had gone out of business (though it continues to defend itself in court).

The court's new decision on copyright was particularly worrisome. It ruled that West headnotes—a few lines of text copying or summarizing a single legal conclusion from a judge's written opinion—could be copyrighted, and that using them to train the ROSS tool was not fair use, in part because ROSS was a competitor to Thomson Reuters. And the court rejected ROSS's attempt to avoid any illegal copying by using a "clean room" procedure often used in software development. The

decision also threatens to limit the public's access to legal texts.

EFF weighed in with an amicus brief joined by the American Library Association, the Association of Research Libraries, the Internet Archive, Public Knowledge, and Public.Resource.Org. We argued that West headnotes are not copyrightable in the first place, since they simply restate individual points from judges' opinions with no meaningful creative contributions. And even if copyright does attach to the headnotes, we argued, the source material is entirely factual statements about what the law is, and West's contribution was minimal, so fair use should have tipped in ROSS's favor. The trial judge had found that the factual nature of the headnotes favored ROSS, but dismissed this factor as unimportant, effectively writing it out of the law.

This case is one of the first to touch on copyright and AI, and is likely to influence many of the other cases that are already pending (with more being filed all the time). That's why we're trying to help the appeals court get this one right. The law should encourage the creation of AI tools to digest and identify facts for use by researchers, including facts about the law.



# Screenshot Showcase


*Posted by tbs, on October 1, 2025, running KDE*

# Wiki Pick:
# Backup & Restore Using Timeshift

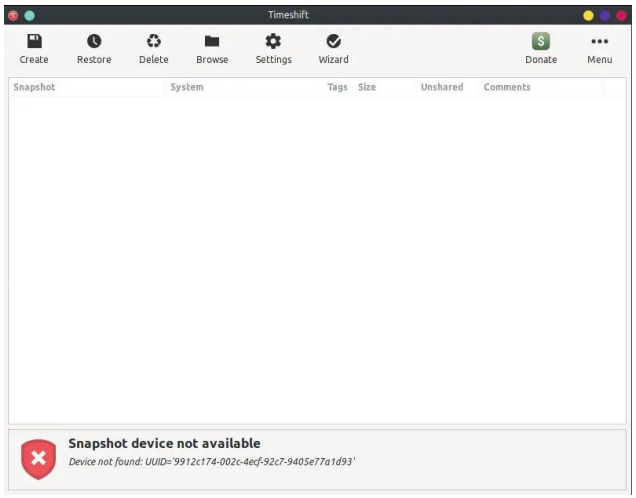
**by The PCLinuxOS Community**

*Relevant to all editions of PCLinuxOS*

**Timeshift** is an application that provides functionality similar to the System Restore feature in Windows and the Time Machine tool in macOS. Timeshift protects your system by taking incremental snapshots of the file system at regular intervals. These snapshots can be restored at a later date to undo all changes to the system. Timeshift is designed to protect **only** system files and settings. User files such as documents, pictures, and music are excluded. This ensures that your user files remain unchanged when you restore your system to an earlier date.

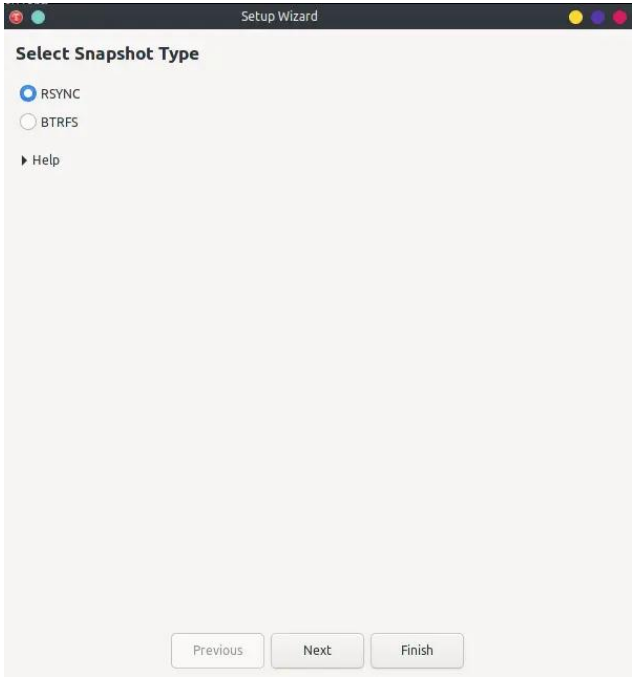
### Installing and running Timeshift

If not already installed on your system, then search in Synaptic for **timeshift** to install Timeshift and its dependencies. Once installed, you will find it on the start menu under **Archiving** > **Timeshift**. You will be prompted for the root password. Enter the root password to continue, and you will then see the main Timeshift window.

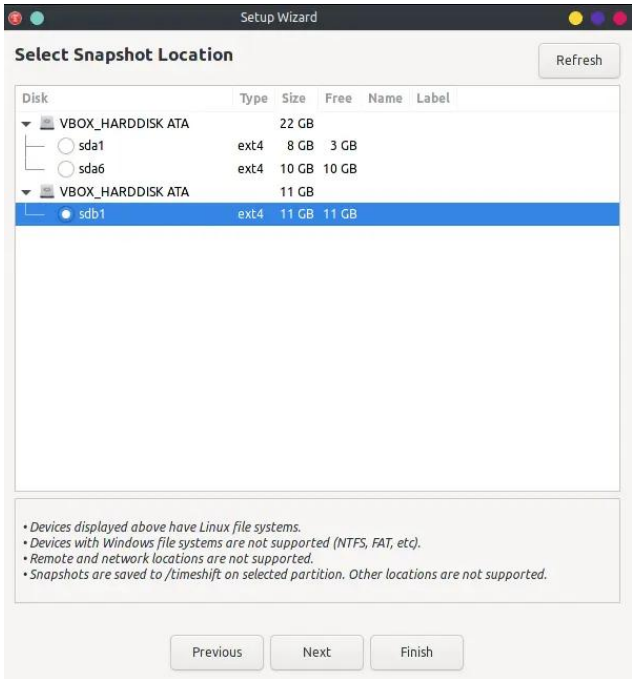



At this point nothing is configured and so the first thing to do is click the **Wizard** button on the toolbar which will walk you through the process of configuring Timeshift snapshots. Timeshift just needs 3 pieces of information: The snapshot type, the location to store the snapshots and optionally a schedule for taking snapshots.

On the first screen, you choose the type of snapshot. Most users should select **RSYNC** as the snapshot type. In RSYNC mode, snapshots are taken using rsync and hard-links. Common files are shared between snapshots, which saves disk space. Each snapshot is a full system backup that can be browsed with a file manager.



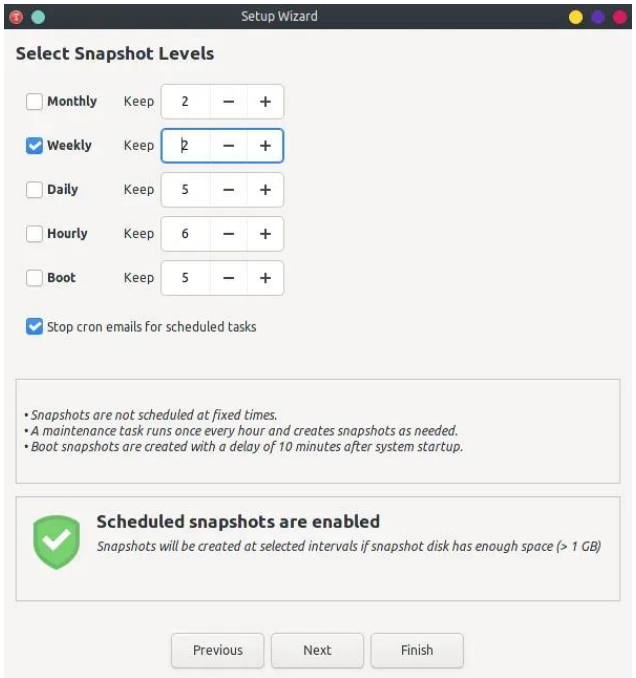

Next, Timeshift will estimate the amount of free space required for creating snapshots and then display a list of disks and partitions available on the system. You can store your snapshots on your main system drive/partition if you wish, but if you want to treat your Timeshift snapshots as normal system backups you should choose a partition on a non-system (external) drive. Timeshift will store the snapshots under / timeshift on the selected partition.




Timeshift will warn if there is not enough free space available on the selected partition. If you only wish to take snapshots manually, then you can click **Finish>** at this point and Timeshift configuration is complete. On the other hand, if you want snapshots taken regularly then click **Next**.

***Note!*** *Snapshots can use a lot of disk space, so make sure you choose a partition with plenty of free space.*

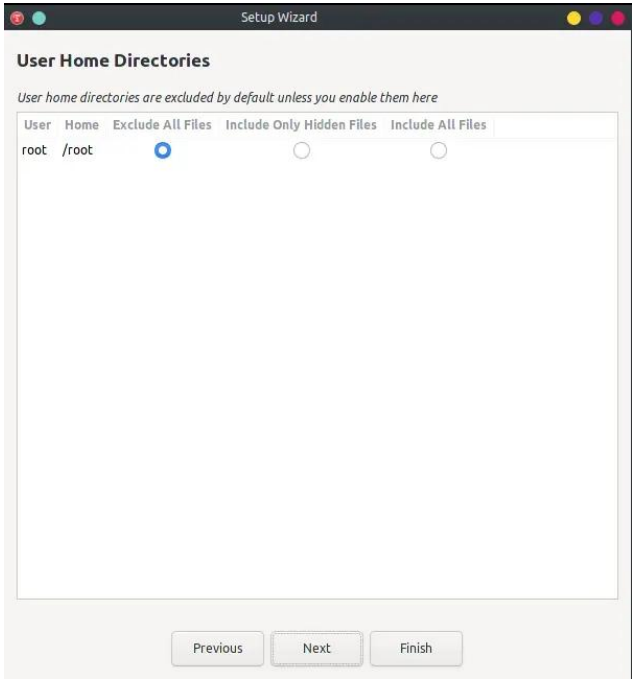
The next screen enables you to choose a schedule for creating snapshots. Here you choose the frequency of the snapshots and the number of snapshots to keep. So on the screen below a snapshot is taken every week, and we keep 2 snapshots which means we have the option of rolling back to last week or the week before.




The **Boot** option takes a snapshot after each reboot (after a delay of 10 minutes in order not to slow down the start-up).

You can choose not to have scheduled snapshots by unticking all the options. In that case, you would create snapshots yourself by clicking the **Create** button on the toolbar, perhaps before doing a system update.

The next screen controls whether the contents of user home directories are included or not. As explained earlier, Timeshift is designed to protect only system files and settings, and so this should be left to **Exclude All Files**. If user directories were to be included, the size of snapshots could quickly get out of hand.

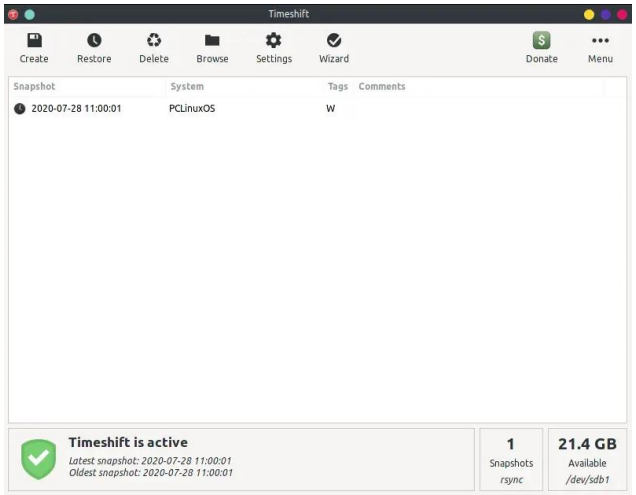



You can now click **Next** or **Finish**. Either way, the setup is complete, and you will be returned to the main screen. If you configured scheduled snapshots, then the current status will be shown at the bottom of the window.


You can change any of the settings by clicking the Settings button on the toolbar.

That is all that is needed to set up Timeshift, and you can now close the Timeshift window. If you have enabled scheduled backups, then within the next hour or so Timeshift will create the first snapshot. Unlike similar tools that take backups at a fixed time of the day, Timeshift is designed to run once every hour and take snapshots only when a snapshot is due. This is more suitable for

users who only have their systems switched on for a few hours daily. Scheduling snapshots at a fixed time would result in missed backups, since the system may not be running when the snapshot is scheduled to run. By running once every hour and creating snapshots when due, Timeshift ensures that backups are not missed.



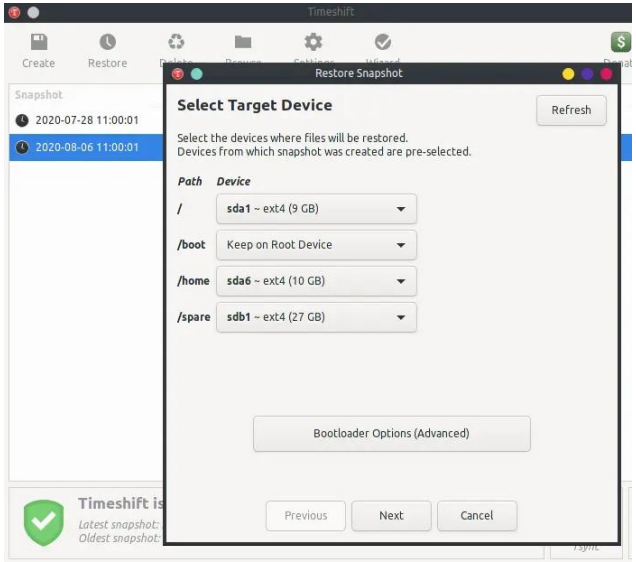

The window lists the available snapshots. The system can be restored back to the time of a snapshot by clicking a snapshot in the window and clicking the **Restore** button on the toolbar. Snapshots can be restored either from the running system (online restore) or from LiveCD/USB if the system is not bootable. Restoring snapshots from the running system requires a reboot to complete the restore process.

***Note!*** *Only systems which use the GRUB2 bootloader are supported.*



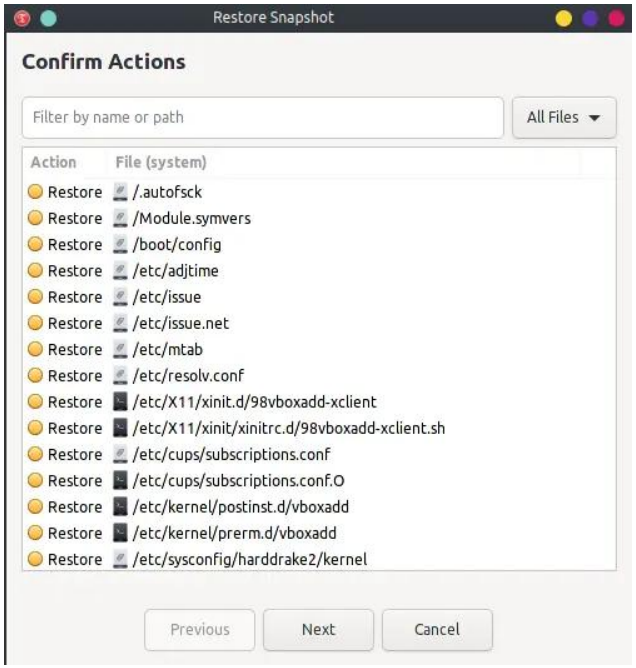
**Restoring snapshots**

The system can be restored back to the time of a snapshot, by clicking a snapshot in the window and clicking the **Restore** button on the toolbar. Snapshots can be restored either from the running system (online restore) or from LiveCD/USB if the system is not bootable. Restoring snapshots from the running system requires a reboot to complete the restore process.




This window shows the disk configuration as it was when the snapshot was taken. There is usually no need to change anything here unless you want to restore to different partitions. Click **Next** and then Timeshift will examine the chosen snapshot to produce a list of files which have changed since the snapshot was taken.






Click **Next** and you will get one final confirmation screen before the restore actually takes place.

**Restoring snapshots using a LiveCD/USB**

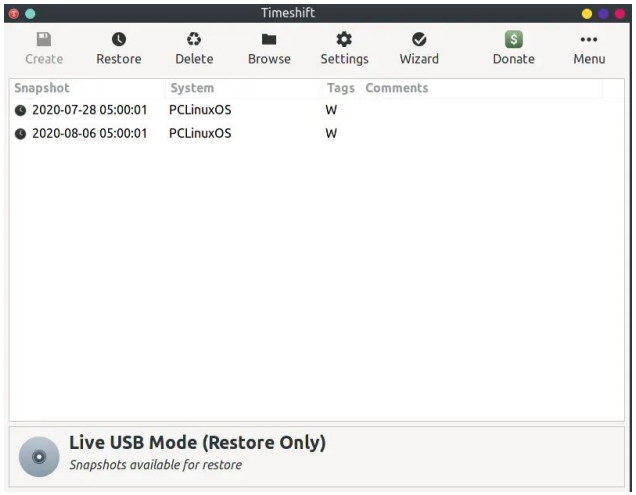
If you are unable to boot your system, you can still restore snapshots by booting a LiveCD/USB and running Timeshift from there.

***Note!*** *If restoring from a LiveCD/USB, you must boot the Live media in the correct mode (Legacy or UEFI) for the installed system.*

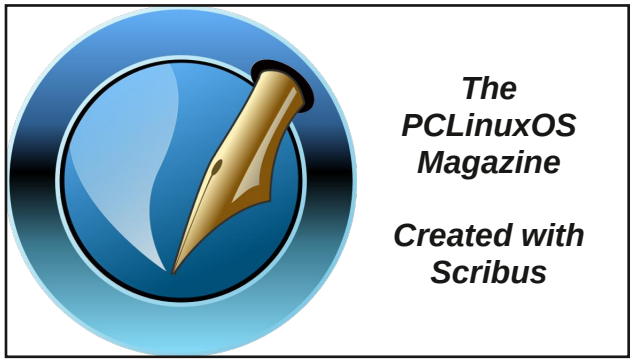
If Timeshift is not installed on the LiveCD/USB, then you can install it in the normal way using Synaptic. When you run Timeshift in this way, it

automatically runs in Live USB mode and only restore functions are available.

Before you can restore, you will need to run the configuration wizard by clicking the **Wizard** button on the toolbar. Then on the Select Snapshot Location screen you should choose the partition where your snapshots are stored and then click **Finish**. You should then see the available snapshots in the main window, and you can continue with Restore as detailed in the previous section.




*You can view the original PCLinuxOS Wiki Knowledgebase article here.*






# Screenshot Showcase

***Posted by piratejumbo, on October 27, 2025, running KDE***

# Tile's Lack Of Encryption Is A Danger For Users Everywhere

**by Thorin Klosowski**
Electronic Frontier Foundation
Reprinted under Creative Commons license

In research shared with Wired, security researchers detailed a series of vulnerabilities and design flaws with Life360's Tile Bluetooth trackers that make it easy for stalkers and the company itself to track the location of Tile devices.

Tile trackers are small Bluetooth trackers, similar to Apple's Airtags, but they work on their own network, not Apple's. We've been raising concerns about these types of trackers since they were first introduced, and provide guidance for finding them if you think someone is using them to track you without your knowledge.

EFF has worked on improving the Detecting Unwanted Location Trackers standard that Apple, Google, and Samsung use, and these companies have at least made incremental improvements. But Tile has done little to mitigate the concerns we've raised around stalkers using their devices to track people.

One of the core fundamentals of that standard is that Bluetooth trackers should rotate their MAC address, making them harder for a third party to track, and that they should encrypt information sent. According to the researchers, Tile does neither.

This has a direct impact on the privacy of legitimate users and opens the device up to potentially even more dangerous stalking. Tile devices do have a rotating ID, but since the MAC address is static and unencrypted, anyone in the vicinity could pick up and track that Bluetooth device.

Other Bluetooth trackers don't broadcast their MAC address, and instead use only a rotating ID, which makes it much harder for someone to record and track the movement of that tag. Apple, Google, and Samsung also all use end-to-end encryption when data about the location is sent to the companies' servers, meaning the companies themselves cannot access that information.

In its privacy policy, Life360 states that, "You are the only one with the ability to see your Tile location and your device location." But if the information from a tracker is sent to and stored by Tile in cleartext (i.e., unencrypted text) as the researchers believe, then the company itself can see the location of the tags and their owners, turning them from single item trackers into surveillance tools.

There are also issues with the "anti-theft mode" that Tile offers. The anti-theft setting hides the

tracker from Tile's "Scan and Secure" detection feature, so it can't be easily found using the app. Ostensibly, this is a feature meant to make it harder for a thief to just use the app to locate a tracker. In exchange for enabling the anti-theft feature, a user has to submit a photo ID and agree to pay a $1 million fine if they're convicted of misusing the tracker.

But that's only helpful if the stalker gets caught, which is a lot less likely when the person being tracked can't use the anti-stalking protection feature in the app to find the tracker following them. As we've said before, it is impossible to make an anti-theft device that secretly notifies only the owner without also making a perfect tool for stalking.

Life360, the company that owns Tile, told Wired it "made a number of improvements" after the researchers reported them, but did not detail what those improvements are.

Many of these issues would be mitigated by doing what their competition is already doing: encrypting the broadcasts from its Bluetooth trackers and randomizing MAC addresses. Every company involved in the location tracker industry business has the responsibility to create a safeguard for people, not just for their lost keys.





# Screenshot Showcase


*Posted by old-polack, on October 2, 2025, running KDE*

# Tip Top Tips: My IP Address

***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.*

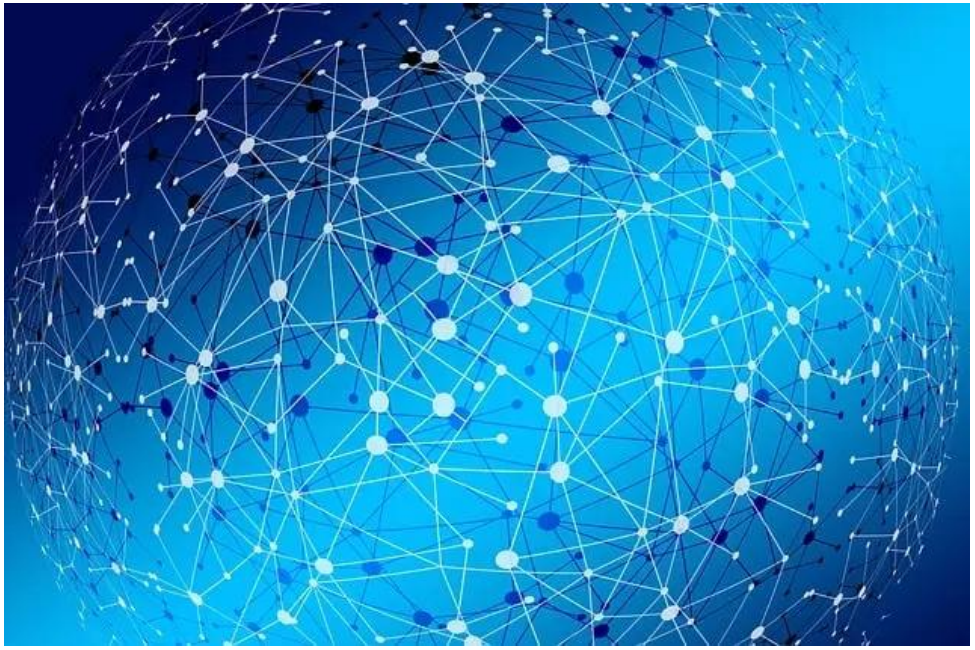


*Image by Gerd Altmann from Pixabay*

This month's tip comes from **SemperOSS**.

Okay, I have been here before with ways to get the current IP address from the command line — but this time, let me show how it can be done from the applications menu on your desktop. It comprises two parts: the actual script, and a .desktop-file that shows up in the menu.

The script depends on the program **dig**, which is part of the standard installation of PCLinuxOS, and the program **zenity**, which can be installed with Synaptic.

The script (called "myip-gui," and stored in "/usr/local/bin"):

```
#! /bin/bash
# Get the IPv4 address
IP="$( /usr/bin/dig +short myip.opendns.com @resolver1.opendns.com
)"
# Set up the initial IPv4-part of the display
Text="<span size=\"xx-large\">$IP"
# Get the IPv6 part if it is enabled
if /sbin/ip -6 a | grep -qP 'inet6 .* scope global'; then
  # Get the IPv6 part
  IP="$( /usr/bin/dig -6 +short AAAA myip.opendns.com
@resolver1.opendns.com )"
  # Append it to the text
  Text+=$'\n'"$IP"
fi
# Close the <span> tag
Text+="</span>"
# Show it on the screen
/usr/bin/zenity --info --text="$Text" --title="My IP" --ok-
label="Close" &
```

And the .desktop file is stored in ".local/share/applications/myip-gui.desktop" in your home directory:

```
[Desktop Entry]
Type=Application
Name=myip
Exec=/usr/local/bin/myip-gui
Terminal=false
Categories=System;Monitor;ConsoleOnly;X-MandrivaLinux-System-
Monitoring;
Keywords=system;process;task
```

Remember that you need to be root to store files in "/usr/local/bin," and that the script must be made executable with the command (again as root) "chmod +x /usr/local/bin/myip-gui". You should now find a menu item called "myip" in the applications menu, in the "More Applications" section.


In a follow-up reply, **Cúig** noted that a user could easily monitor their IP address from either of two commands on the command line: **curl ifconfig.co/ip** and/or **curl ip.me**.

He also pointed out that you could put it all into a desktop file if that is what is needed, without even creating a script, like below:

```
[Desktop Entry]
Categories=X-MandrivaLinux-System-Archiving;
Comment=Display my WAN IP Address
Exec=MyIP=$(curl ifconfig.co/ip); zenity --info --width=150 --
text=$MyIP --title="My WAN IP" --ok-label=Close &
GenericName=MyIP
Icon=internet-web-browser
Keywords=MyIP;
MimeType=
Name=MyIP
Path=
StartupNotify=true
Terminal=false
Type=Application
```

**SemperOSS** replied that yes, it is easier, indeed, but pointed out that many (most?) are not comfortable using the command line if avoidable … and it works too — but misses an opportunity to show a bit of bash scripting if people are interested.

He also pointed out that it could even be simplified by changing the Exec line to:

```
Exec=zenity --info --text="$(curl ifconfig.co/ip)" --title="My WAN
IP" --ok-label=Close &
```

which (with the extra quotes), also handles the case of the website spitting something unexpected out containing spaces.

# Flock's Gunshot Detection Microphones Will Start Listening For Human Voices

**by Matthew Guariglia**
Electronic Frontier Foundation


Flock Safety, the police technology company most notable for their extensive network of automated license plate readers spread throughout the United States, is rolling out a new and troubling product that may create headaches for the cities that adopt it: detection of "human distress" via audio. As part of their suite of technologies, Flock has been pushing Raven, their version of acoustic gunshot detection. These devices capture sounds in public places and use machine learning to try to identify gunshots and then alert police — but EFF has long warned that they are also high-powered microphones parked above densely-populated city streets. Cities now have one more reason to follow the lead of many other municipalities and cancel their Flock contracts, before this new feature causes civil liberties harms to residents and headaches for cities.

In marketing materials, Flock has been touting new features to their Raven product—including the ability of the device to alert police based on sounds, including "distress." The online ad for the product, which allows cities to apply for early access to the technology, shows the image of police getting an alert for "screaming." (Since the publication of this blog post, Flock has quietly amended the ad on this webpage to say "distress" instead of "screaming").

It's unclear how this technology works. For acoustic gunshot detection, generally the microphones are looking for sounds that would signify gunshots (though in practice they often mistake car backfires or fireworks for gunshots). Flock needs to come forward now with an explanation of exactly how their new technology functions. It is unclear how these devices will interact with state "eavesdropping" laws that limit listening to or recording the private conversations that often take place in public.

Flock is no stranger to causing legal challenges for the cities and states that adopt their products. In Illinois, Flock was accused of violating state law by allowing Immigration and Customs Enforcement (ICE), a federal agency, access to license plate reader data taken within the state. That's not all. In 2023, a North Carolina judge halted the installation of Flock cameras statewide for operating in the state without a license. When the city of Evanston, Illinois recently canceled its contract with Flock, it ordered the company to take down their license plate readers – only for Flock to mysteriously reinstall them a few days later. This city has now sent Flock a cease and desist order and, in the meantime, has put black tape over the cameras. For some, the technology isn't worth its

mounting downsides. As one Illinois village trustee wrote while explaining his vote to cancel the city's contract with Flock, "According to our own Civilian Police Oversight Commission, over 99% of Flock alerts do not result in any police action."

Gunshot detection technology is dangerous enough as it is — police showing up to alerts they think are gunfire only to find children playing with fireworks is a recipe for innocent people to get hurt. This isn't hypothetical: in Chicago, a child really was shot at by police who thought they were responding to a shooting thanks to a ShotSpotter alert. Introducing a new feature that allows these pre-installed Raven microphones all over cities to begin listening for human voices in distress is likely to open up a whole new can of unforeseen legal, civil liberties, and even bodily safety consequences.





# Screenshot Showcase


*Posted by mutse, on October 28, 2025, running Mate.*

# PCLinuxOS Recipe Corner Bonus


## Slow Cooker Sesame Chicken with Cashews

Serves 4

**INGREDIENTS:**

1/4 cup plus 2 tablespoons Progresso™ chicken broth (from 32-oz carton)
1/4 cup honey
1/4 cup soy sauce
1 tablespoon unseasoned rice vinegar
2 teaspoons toasted sesame oil
1-inch piece fresh gingerroot, peeled and grated
4 teaspoons finely chopped fresh garlic
1/4 teaspoon crushed red pepper flakes
1 package (20 oz) boneless skinless chicken thighs, cut into 2-inch pieces
2 tablespoons cornstarch
4 cups small fresh broccoli florets
1/2 cup salted roasted whole cashews
2 teaspoons toasted sesame seed
Sliced green onions, if desired
Cooked white rice, if desired

**DIRECTIONS:**

Spray 3 1/2- to 4-quart slow cooker with cooking spray. In a medium bowl, mix 1/4 cup chicken broth, the honey, 2 tablespoons of the soy sauce, the rice vinegar, sesame oil, gingerroot, garlic and red pepper. Add chicken and mix to coat; transfer to slow cooker.

Cover; cook on Low heat setting 2 to 2 1/2 hours or until chicken is no longer pink. In a small bowl, mix cornstarch and remaining 2 tablespoons of chicken broth; stir into a slow cooker. Cover; cook on High heat setting 15 to 20 minutes or until bubbly around edges and starting to thicken.

Add remaining 2 tablespoons soy sauce and the broccoli to the slow cooker, mixing to coat broccoli with sauce mixture; cover and continue cooking 10 to 15 minutes or until broccoli is crisp-tender. Stir in cashews. Before serving, sprinkle with sesame seed, and garnish with sliced green onions. Serve with cooked white rice.

**NUTRITION:**

Calories: 430 Carbs: 33g Sodium: 710mg
Fiber: 3g Protein: 36g

# PCLinuxOS Puzzled Partitions

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

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

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

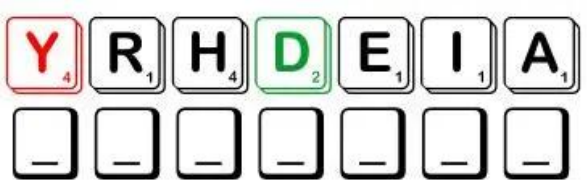
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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.

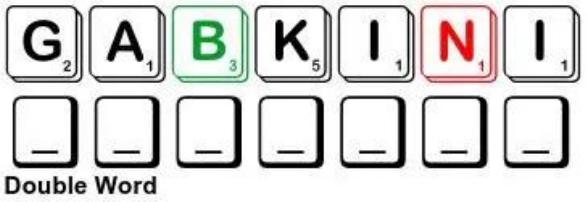
**SCRAPPLER RULES:**

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 240, average score 168.**

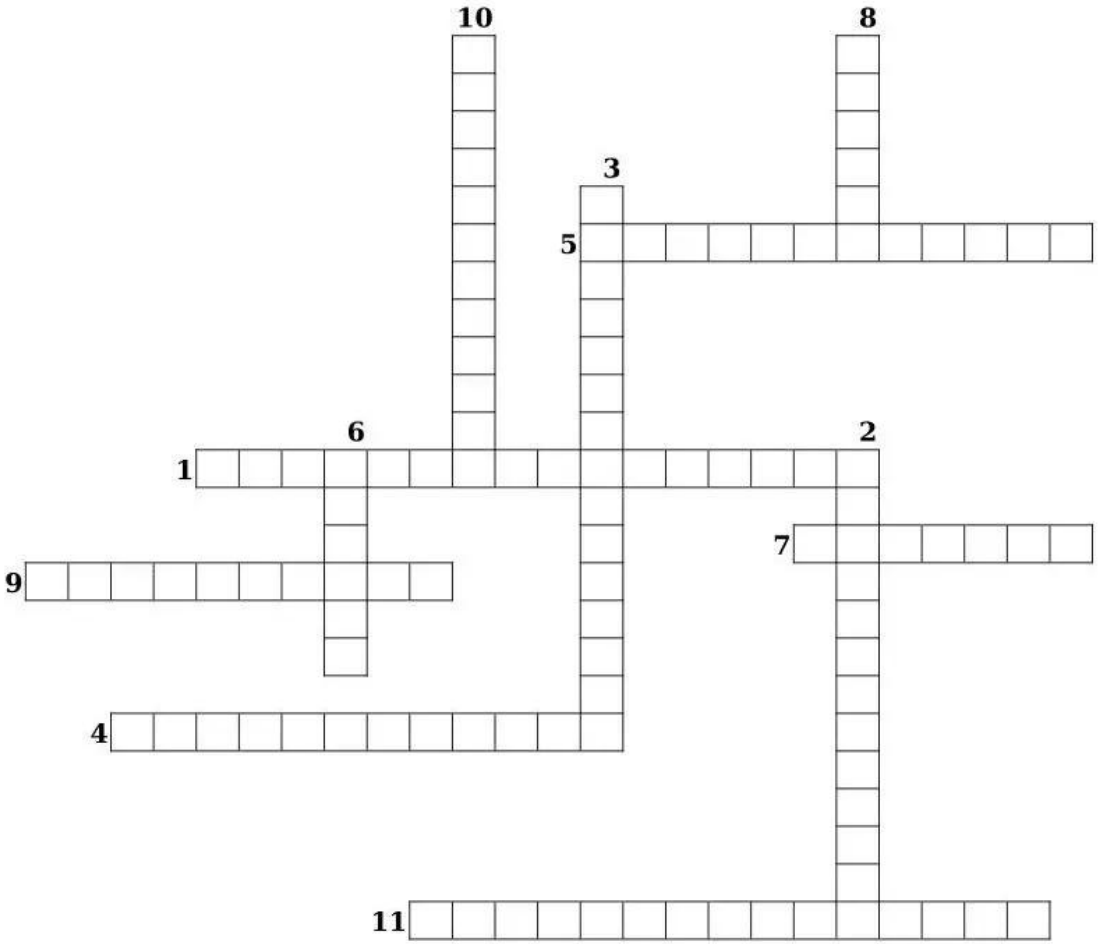
# November 2025 Word Find
# Fall Activities

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

APPLE PICKING
BAKING
BIRD WATCHING
BOBBING FOR APPLES
BONFIRE NIGHT
CAMPFIRE STORYTELLING
CARRIAGE RIDE
CIDER TASTING
FALL FESTIVALS
FOLIAGE DRIVE
FOOTBALL GAME
HARVEST FESTIVAL
HAYRIDE
HIKING
HORSEBACK RIDING
MAKING CIDER
NATURE SCAVENGER HUNT
ORCHARD VISIT
SCENIC TRAIN RIDE
TAILGATING
WINE TASTING

**Download Puzzle Solutions Here**

# November 2025 Crossword
# Fall Activities




1. A game where the goal is to remove an apple from a tub of water using only your mouth.
2. A playful game where players search for specific items, complete challenges, or follow creative clues to win.
3. A leisurely, tourist-focused journey that operates on a special railway to showcase beautiful landscapes.
4. A scenic car trip, often in the autumn, taken to view the changing colors of tree leaves.
5. A service whereby a carriage, drawn by a horse controlled by a driver, is made available to the public for a fee.
6. The action of cooking food by dry heat without direct exposure to a flame
7. A social event in which a group of people go for a ride in an open vehicle filled with hay
8. The activity of going for long walks, especially in the country or woods.
9. A social gathering at which an informal meal is served from the back of a parked vehicle.
10. The practice of observing birds in their natural environment as a hobby.
11. A celebration of the annual harvest, especially (in Britain) one held in schools.

**Download Puzzle Solutions Here**

# Mixed-Up-Meme Scrambler

SELBS _ _ _ _ _

DRUFA _ _ _ _ _

FIMSIT _ _ _ _ _ _

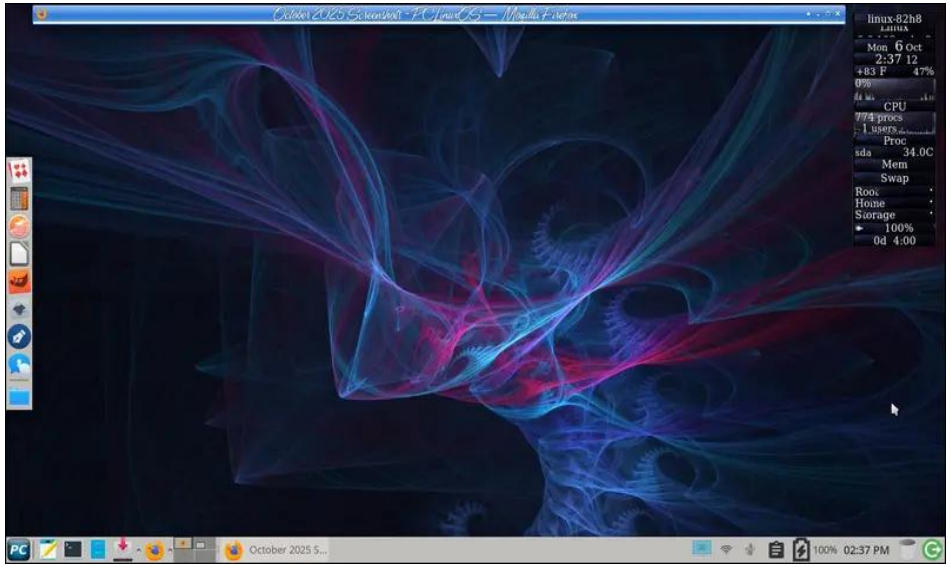
DEBISE _ _ _ _ _ _

The turkey and the family were this on Thanksgiving...

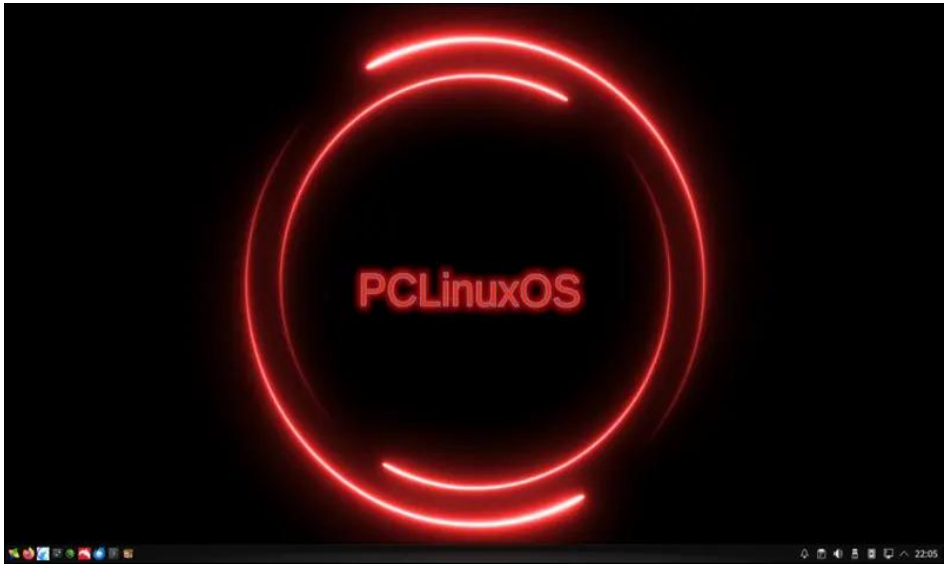
" _ _ _ _ _ _ _ _ "

Download Puzzle Solutions Here

# More Screenshot Showcase

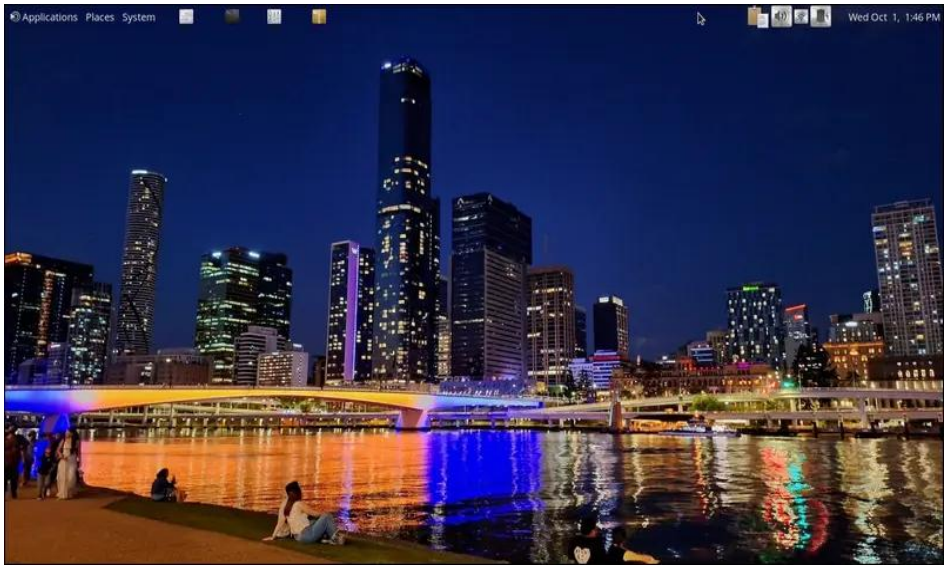



*Posted by Meemaw, on October 6, 2025, running Xfce.*




*Posted by luikki, on October 1, 2025, running KDE.*


*Posted by francescoinblack, on October 5, 2025, running icewm.*




*Posted by brisvegas, on October 1, 2025, running Mate.*