The PCLinuxOS magazine

Volume 221

June, 2025

In This Issue...

The PCLinuxOS magazine

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

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

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)
Assistant Editor: Meemaw
Artwork: Paul Arnote, Meemaw
PDF Layout: Paul Arnote, Meemaw
HTML Layout: tbs

Staff:
YouCanToo
David Pardue
Alessandro Ebersol

Contributors:
David Marshall

From The Chief Editor's Desk

“There’s an app for that.”

When smartphones first appeared on the scene nearly 20 years ago, those words were greeted with great enthusiasm. Today, that phrase is dreaded.

I’m talking about app fatigue. It’s a very real phenomenon.

It seems like everyone and their brother, sister, mother, father, aunt, uncle, cousin, grandparent, and acquaintance has their own dedicated app. Enough already!

Around my parts, there are WAY too many separate apps for goods and services. Do you want the best buy on a Subway submarine sandwich? You’ll have to download Subway’s app, because the best buys are ONLY available to those who use the Subway app. If you want that $6.99 footlong sandwich, that price is only available when you order through their app. Do you want a great buy on a Wendy’s hamburger? You’ll have to download Wendy’s dedicated app. And thus it continues across a wide range of dedicated apps.

There are apps where the best prices are only available to the user of a particular app. Other apps offer exclusive “deals” only to users of their dedicated app. If you don’t have THEIR app, you get the honor of paying the higher price.

When I go to a MLB game, there’s an app for that. Since the pandemic, there are no more physical tickets. Your tickets are stored electronically on your smartphone. If you go to the concession stand to purchase the exorbitantly priced food and drink items, you can only pay with a credit/debit card, or with a payment app on your phone. No cash is allowed. They call it “contactless payment.” If you download the “Ballpark” app, you can get in-game discounts on upgraded seats and other discounted services. Oh yeah. That’s right. You must download the “Ballpark” app, because that’s where your tickets for admittance to the stadium are stored. And, take it from me: everything you do in the baseball stadium is very closely monitored and recorded. This was apparent after we attended a special event this year when the Kansas City Royals hosted a day for Scouts. In the days following the game, I got all kinds of emails, as well as notifications on my phone.

Consider for a moment all of the problems and pitfalls with this approach of everyone having their own dedicated app.

First, there’s the overwhelming number of apps that a “normal” person would have to install on their smartphone. EVERYONE has their own dedicated app. Given the bloat of many of these apps, there’s a very real chance that you could quickly run out of storage space on your smartphone.

Then, there’s the security and privacy issues. Do you know what information is being sent from any particular smartphone app back to its “command base?” Probably not. Most people do not pay attention to the “permissions” granted to each individual app that they install on their smartphone, let alone what data is shared and with whom. This places things like contact lists, geolocation, photos, documents … just about anything stored on your smartphone … at risk. That’s placing an awful lot of “trust” in the app creator that they don’t funnel all of your available data to some central “command” server. Of course, each app installed increases the risk of a virus or other security vulnerability, as well.

Most users probably couldn’t care less. They blindly and blissfully just install these apps without giving any regard to their security or the security of their data (if they were truly concerned about their privacy, they wouldn’t be on platforms like Facebook and X to start with). And then, they get to endure all of the “push notifications” that typically come with these apps. Frankly, I don’t have the patience or stomach to deal with all of those interruptions. And, with private personal data being vacuumed up by every entity on the planet like a herd of animals on a voracious feeding frenzy, I’m not all that eager to give up my privacy and the security of my data. It’s NONE OF THEIR BUSINESS where I go, what I do when I’m there, who I do it with, who I talk to, when I do it, what websites I visit and when, or any other datasets collected by these so-called “smartphones.”

Whenever I have the choice, I prefer to use my computer over my smartphone. At least with my computer, I have a lot more control over my data and how I secure it. I simply do not have anything close to that level of control of my data on a smartphone. Unfortunately, there are times when I must use the apps on my smartphone (like when I attend a Kansas City Royals game).

Yep. I’m there. I’ve reached my threshold for “app fatigue.”

****

This month’s cover image comes from PCLinuxOS’s resident shutterbug, **The CrankyZombie**. With Spring in full swing, his image of the Yellow Flag Iris (a.k.a. the Bog Iris) seemed fitting.

****

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

Screenshot Showcase

Posted by brisvegas, May 1, 2025, running Mate.

The U.S. Copyright Office's Draft Report On AI Training Errs On Fair Use

by Tori Noble, Mitch Stoltz, and Corynne McSherry
Electronic Frontier Foundation

Within the next decade, generative AI could join computers and electricity as one of the most transformational technologies in history, with all of the promise and peril that implies. Governments' responses to GenAI—including new legal precedents—need to thoughtfully address real-world harms without destroying the public benefits GenAI can offer. Unfortunately, the U.S. Copyright Office's rushed draft report on AI training misses the mark.

The Report Bungles Fair Use

Released amidst a set of controversial job terminations, the Copyright Office's report covers a wide range of issues with varying degrees of nuance. But on the core legal question — whether using copyrighted works to train GenAI is a fair use—it stumbles badly. The report misapplies long-settled fair use principles and ultimately puts a thumb on the scale in favor of copyright owners at the expense of creativity and innovation.

To work effectively, today's GenAI systems need to be trained on very large collections of human-created works—probably millions of them. At this scale, locating copyright holders and getting their permission is daunting for even the biggest and wealthiest AI companies, and impossible for smaller competitors. If training makes fair use of copyrighted works, however, then no permission is needed.

Right now, courts are considering dozens of lawsuits that raise the question of fair use for GenAI training. Federal District Judge Vince Chhabria is poised to rule on this question, after hearing oral arguments in Kadrey v. Meta Platforms. The Third Circuit Court of Appeals is expected to consider a similar fair use issue in Thomson Reuters v. Ross Intelligence. Courts are well-equipped to resolve this pivotal issue by applying existing law to specific uses and AI technologies.

Courts Should Reject the Copyright Office's Fair Use Analysis

The report's fair use discussion contains some fundamental errors that place a thumb on the scale in favor of rightsholders. Though the report is non-binding, it could influence courts, including in cases like Kadrey, where plaintiffs have already filed a copy of the report and urged the court to defer to its analysis.

Courts need only accept the Copyright Office's draft conclusions, however, if they are persuasive. They are not.

The Office’s fair use analysis is not one the courts should follow. It repeatedly conflates the use of works for training models—a necessary step in the process of building a GenAI model—with the use of the model to create substantially similar works. It also misapplies basic fair use principles and embraces a novel theory of market harm that has never been endorsed by any court.

The first problem is the Copyright Office’s transformative use analysis. Highly transformative uses—those that serve a different purpose than that of the original work—are very likely to be fair. Courts routinely hold that using copyrighted works to build new software and technology—including search engines, video games, and mobile apps—is a highly transformative use because it serves a new and distinct purpose. Here, the original works were created for various purposes, and using them to train large language models is surely very different.

The report attempts to sidestep that conclusion by repeatedly ignoring the actual use in question —training —and focusing instead on how the model may be ultimately used. If the model is ultimately used primarily to create a class of works that are similar to the original works on which it was trained, the Office argues, then the intermediate copying can’t be considered transformative. This fundamentally misunderstands transformative use, which should turn on whether a model itself is a new creation with its own distinct purpose, not whether any of its potential uses might affect demand for a work on which it was trained—a dubious standard that runs contrary to decades of precedent.

The Copyright Office’s transformative use analysis also suggests that the fair use analysis should consider whether works were obtained in “bad faith,” and whether developers respected the right “to control” the use of copyrighted works. But the Supreme Court is skeptical that bad faith has any role to play in the fair use analysis, and has made clear that fair use is not a privilege reserved for the well-behaved. And rightsholders don’t have the right to control fair uses—that’s kind of the point.

Finally, the Office adopts a novel and badly misguided theory of “market harm.” Traditionally, the fair use analysis requires courts to consider the effects of the use on the market for the work in question. The Copyright Office suggests instead that courts should consider overall effects of the use of the models to produce generally similar works. By this logic, if a model was trained on a Bridgerton novel—among millions of other works—and was later used by a third party to produce romance novels, that might harm series author Julia Quinn’s bottom line.

This market dilution theory has four fundamental problems. First, like the transformative use analysis, it conflates training with outputs. Second, it’s not supported by any relevant precedent. Third, it’s based entirely on speculation that Bridgerton fans will buy random “romance novels” instead of works produced by a bestselling author they know and love. This relies on breathtaking assumptions that lack evidence, including that all works in the same genre are good substitutes for each other—regardless of their quality, originality, or acclaim. Lastly, even if competition from other, unique works might reduce sales, it isn’t the type of market harm that weighs against fair use.

Nor is lost revenue from licenses for fair uses a type of market harm that the law should recognize. Prioritizing private licensing market “solutions” over user rights would dramatically expand the market power of major media companies and chill the creativity and innovation that copyright is intended to promote. Indeed, the fair use doctrine exists in part to create breathing room for technological innovation, from the phonograph record to the videocassette recorder to the internet itself. Without fair use, crushing copyright liability could stunt the development of AI technology.

We’re still digesting this report, but our initial review suggests that, on balance, the Copyright Office’s approach to fair use for GenAI training isn’t a dispassionate report on how existing copyright law applies to this new and revolutionary technology. It’s a policy judgment about the value of GenAI technology for future creativity, by an office that has no business making new, free-floating policy decisions.

The courts should not follow the Copyright Office’s speculations about GenAI. They should follow precedent.

ICYMI: China-linked Cyber Espionage Group Compromise Multiple Organizations In SE Asia

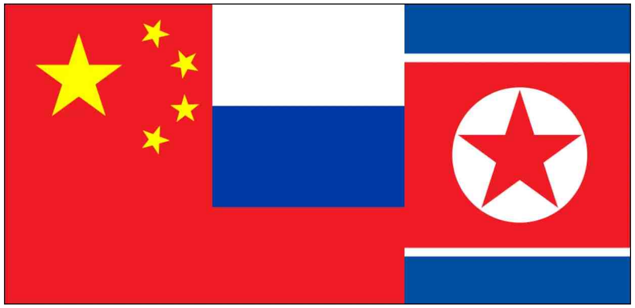
by Paul Arnote (parnote)

Image by Gerd Altmann from Pixabay

A known data breach affecting a major insurance administrator may have compromised the personal information of nearly twice as many people as previously reported, according to an article from Lifehacker. A May 2024 cyberattack on Landmark Admin is believed to include at least 1.6 million people's data, according to an updated filing with the Maine attorney general's office. Landmark Admin is a Texas-based third-party administrator (TPA) for life insurance and annuity companies like Liberty Bankers Life and American Benefit Life, which offer policies nationwide. A TPA offers insurers support with accounting, regulatory reporting, reinsurance, and IT. That means that while you may not ever have dealt directly with Landmark Admin, your information could still have been leaked.

HP Inc. has agreed to pay $4 million to settle a class-action lawsuit in the US that alleged it used deceptive pricing tactics on its website, including fake discounts and misleading limited-time offers, according to an article from The Register. As a result, customers who bought specific PC models [PDF], as well as some mice and keyboards, between June 5, 2021, and October 28, 2024, may be able to get a few bucks back, assuming the judge approves the settlement and affected customers file the necessary claim form. HP did not admit any wrongdoing as part of the deal. The dispute began on September 7, 2021, when Rodney Carvalho purchased a desktop PC from HP Inc's website for $899.99, advertised as $100 off the regular price of $999.99. However, he alleged in a lawsuit – brought against the computer titan in California a year later – that HP had been selling the same model at $899.99 for months, making the advertised discount misleading.

In a rather clever attack, hackers leveraged a weakness that allowed them to send a fake email that seemed delivered from Google's systems, passing all verifications but pointing to a fraudulent page that collected logins, according to an article from Bleeping Computer. The attacker leveraged Google's infrastructure to trick recipients into accessing a legitimate-looking "support portal" that asks for Google account credentials. The fraudulent message appeared to come from "no-reply@google.com" and passed the DomainKeys Identified Mail (DKIM) authentication method, but the real sender was different.



The China-linked cyber espionage group tracked as Lotus Panda has been attributed to a campaign that compromised multiple organizations in an unnamed Southeast Asian country between August 2024 and February 2025, according to an article from The Hacker News. "Targets included a government ministry, an air traffic control organization, a telecoms operator, and a construction company," the Symantec Threat Hunter Team said in a new report shared with The Hacker News. "The attacks involved the use of multiple new custom tools, including loaders, credential stealers, and a reverse SSH tool." The intrusion set is also said to have targeted a news agency located in another country in Southeast Asia and an air freight organization located in another neighboring country.

The European Union is determined to enforce its full digital rule book no matter who is in charge of companies such as X, Meta, Apple, and TikTok or where they are

based, Commission President Ursula von der Leyen told Politico, according to an article from Reuters. “That's why we've opened cases against TikTok, X, Apple, Meta just to name a few. We apply the rules fairly, proportionally, and without bias. We don't care where a company's from and who's running it. We care about protecting people,” Politico quoted von der Leyen as saying on Sunday.

Notion Mail is finally out in the wild, for anyone who has a Gmail account, according to an article from Lifehacker. And it's quintessential Notion. If you've used the standard Notion app, you really can't confuse it for anything else. Notion Mail is a minimalist and text-based take on the Mail app that isn't trying to do anything revolutionary. There are no AI summaries, and no complicated split views like in Superhuman. It's just your email, sorted in a way that you like. What does it mean, though, to apply the Notion philosophy to email, and is it good enough for you to make the switch? That is, if you even can. Currently, Notion Mail only works on the Web and on Mac, and it only supports Gmail accounts (leaving out Outlook and enterprise emails). Notion Mail's iOS app is on the way, and the Android app will launch in 2025 as well. But there's no app for Windows on the roadmap.

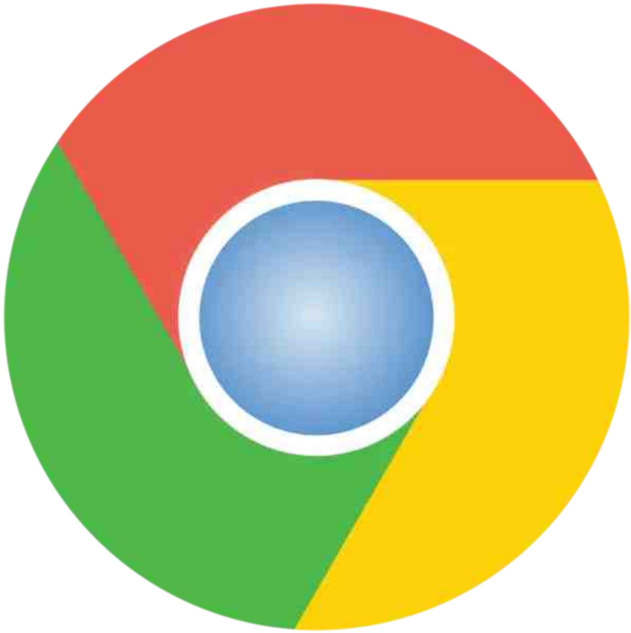
Image by Gerd Altmann from Pixabay

Blue Shield of California disclosed it suffered a data breach after exposing protected health information of 4.7 million members to Google's analytics and advertising platforms, according to an article from Bleeping Computer. The nonprofit health plan, which serves nearly 6 million members across California, published a data breach notification on its website stating that member data was exposed between April 2021 and January 2024. In late April 2025, the United States Department of Health and Human Services breach portal was updated to state that the leak exposed 4.7 million members' protected health data. According to the notice, the exposure was caused by a misconfiguration of Google Analytics on certain Blue Shield sites. This resulted in the sensitive data potentially being shared with Google advertising platforms and advertisers.

It looks like Google Photos is rolling out the ability to convert standard photos into Ultra HDR after they’ve been taken, according to an article from Android Authority. The feature seems to have started appearing for some users. Google Photos has been working on an “Ultra HDR” editing feature for a while now. We first spotted signs of the feature in the app last September, but at the time, the option wasn’t functional, and it wasn’t clear what it was supposed to do. Still, we had a hunch it was tied to the Ultra HDR file format Google introduced with Android 14. Ultra HDR allows for capturing and displaying photos with a wider range of light and color. The result is more vibrant, lifelike images, especially noticeable on devices with high dynamic range (HDR) displays. But Ultra HDR is also backward-compatible, meaning it can still display normally on older, non-HDR devices. It does this by packing both SDR and HDR versions of the image into a single file.

In a surprising twist at Google’s ongoing antitrust trial, an OpenAI executive revealed that the company would be interested in buying Google’s Chrome browser if

regulators force its sale, according to an article from TechRepublic. The bombshell statement came as the US government pushes for drastic measures to break up Google's dominance in online search. Nick Turley, head of product for ChatGPT, testified in court on Tuesday that OpenAI would jump at the chance to acquire Chrome if it ever hits the market. "Yes, we would, as would many other parties," Turley said, according to Bloomberg. He added that owning Chrome could help OpenAI create an "AI-first" browsing experience, offering users something truly unique.



Google has made an unusual announcement about browser cookies, but it may not come as much of a surprise given recent events, according to an article from Ars Technica. After years spent tinkering with the Privacy Sandbox, Google has essentially called it quits. According to Anthony Chavez, VP of the company's Privacy Sandbox initiative, Google won't be rolling out a planned feature to help users disable third-party cookies. Instead, cookie support will remain in place as is, possibly forever. Beginning in 2019, Google embarked on an effort under the Privacy Sandbox banner aimed at developing a new way to target ads that could preserve a modicum of user privacy. This approach included doing away with third-party cookies, small snippets of code that advertisers use to follow users around the web. Google struggled to find a solution that pleased everyone. Its initial proposal for FLoC (Federated Learning of Cohorts) was widely derided as hardly any better than cookies. Google then moved on to the Topics API, but the company's plans to kill cookies have been delayed repeatedly since 2022. Until today, Google was still planning to roll out a dialog in Chrome that would prompt users to turn off third-party cookies in favor of Google's updated solution. According to Chavez, Google has been heartened to see the advertising industry taking privacy more seriously. As a result, Google won't be pushing that cookie dialog to users. Users can still choose to disable third-party cookies in Chrome, though.

Data breaches targeting healthcare and compromising patient information seem to be coming fast and furious, the latest of which occurred at Yale New Haven Health (YNHHS), a massive nonprofit healthcare network in Connecticut. **Hackers stole the data of more than 5.5 million individuals during an attack in March 2025**, according to an article from Lifehacker. The organization discovered "unusual activity" on its system on March 8, 2025, which was later identified as unauthorized third-party access that allowed bad actors to copy certain patient data. While the information stolen varies by individual, it may include name, date of birth, address, phone number, email address, race, ethnicity, Social Security number, patient type, and medical record number. YNHHS says the breach did not include access to medical records, treatment information, or financial data (such as account and payment information).

DuckDuckGo may face a user backlash after security researchers discovered a hidden tracking agreement with Microsoft, according to an article from TechRadar. The privacy-focused company offers a search engine that claims not to track people's searches, or behavior, and also doesn't build user profiles that can be used to display personalized advertising. Search engine aside, DuckDuckGo also offers a mobile browser of the same name, but this has raised concerns, as although this promises to block hidden third-party trackers, some from a certain tech giant are allowed to continue operating. Namely, while Google's and Facebook's trackers are being blocked, those of Microsoft are allowed to continue running. Zach Edwards, the security researcher who first discovered the issue, later also found that trackers related to the bing.com and linkedin.com domains were also being allowed through the blocks. The news quickly drew in crowds of dissatisfied users, with DuckDuckGo founder and CEO Gabriel Weinberg, soon chiming in to confirm the authenticity of the findings. Apparently, DuckDuckGo has a search syndication agreement with the software giant from Redmond, with Weinberg adding that the restrictions are only found in the browser, and are not related to the search engine. What remains unknown is why the company who is known for its transparency decided to keep this agreement a secret for as long as it could.

The European Union has fined Apple and Meta a combined $800 million for violating its antitrust laws. The bloc took issue with Apple's restrictions on app developers informing users about offers outside the App Store and Meta's advertising model, which compels users to pay to prevent their data from being sold to advertisers, according to an article from TechRepublic. Both companies were formally charged last summer for these violations of the Digital Markets Act, and the fines are the first under the 2022 legislation. The act aims to promote fairness and competition among digital products and services by enforcing rules on certain influential tech firms, called "gatekeepers." Apple and Meta now have 60 days to comply or could face additional penalties. Fines for DMA breaches can be up to 10% of a company's total worldwide turnover, or 20% for repeated offences, but those handed to Apple and Meta are nowhere near this.

A new study in which artificial intelligence outperformed expert virologists in specialized laboratory tasks is raising hopes for faster biomedical breakthroughs and fears about bioweapon risks, according to an article from eWeek. Researchers tested leading AI models against the Virology Capabilities Test, a benchmark designed to assess expert-level knowledge in virology and wet lab protocols. The results suggest that AI models like OpenAI's GPT-4o surpassed the accuracy of most human virologists.

According to an article from Reuters, **Apple aims to make most of its iPhones sold in the United States at factories in India by the end of 2026, and is speeding up those plans to navigate potentially higher tariffs in China**, its main manufacturing base, a source told Reuters. The U.S. tech giant is holding urgent talks with contract manufacturers Foxconn and Tata to achieve that goal, the person, who declined to be named as the planning process is confidential, said on April 25.

Image by Andreas Grönberg from Pixabay

OpenAI, Perplexity, and Yahoo have expressed an interest in possibly buying Chrome if Google's browser is for sale, according to an article from TechRepublic. With roughly two-thirds of the global browser market, Chrome is the default browser for billions of users. That's why OpenAI, Perplexity, and even Yahoo see it as a golden opportunity. Owning Chrome would give any company instant access to a massive audience, letting them push their own search engines, AI tools, or other services. Nick Turley, head of product at OpenAI, testified that his company would be eager to buy Chrome if it becomes available. "Yes, we would, as would many other parties," Turley said in court. He added that owning Chrome could help OpenAI build an "AI-first" browsing experience. AI search startup Perplexity is also interested in buying Chrome. Dmitry Shevelenko, Perplexity's chief business officer, said, "I think we could do it" when asked if Perplexity could run Chrome without sacrificing quality, according to The Verge. Perplexity is already working on its own browser, but buying Chrome would be a shortcut to billions of users. Yahoo is another potential buyer. Brian Provost, Yahoo Search's general manager, testified that buying Chrome would cost "tens of billions of dollars" but said it could happen with backing from Apollo Global Management, Yahoo's owner, The Verge reported.

Amazon's Kuiper broadband internet constellation is starting to take shape, with its first batch of satellites shipped and deployed into space on April 28, according to an article from The Verge. The launch is just the first of 80 that Amazon has lined up to take all 3,236 Project Kuiper satellites into low-Earth orbit as part of the retail giant's effort to compete with Starlink — SpaceX's market-dominating satellite internet business. The United Launch Alliance (ULA) Atlas V rocket carrying Amazon's first 27 Kuiper satellites was launched from Florida's Cape Canaveral Space Force Station at 7PM ET on April 28th, after its first attempt on April 9th was scrubbed due to poor weather conditions.

In February, It's Foss News reported that a WSL image for Arch Linux was on its way, and as of now, it has become official — Arch Linux is available, according to an article from ZDNet. Windows Subsystem for Linux is a compatibility layer that allows the running of a full-blown Linux environment. Up until this point, the only images available for WSL have been Ubuntu, Debian, Fedora Remix, openSUSE, Kali Linux, and Pengwin. The addition of Arch delivers a rolling release distribution that should excite plenty of users, developers, and admins who want to finally try Arch.

Image by Julian Di Pietrantonio from Pixabay

Apple sent spyware alerts to users in 100 countries. If you received one, don't ignore it, according to an article from Lifehacker. As much as this situation sounds like classic spam, it's very much not: Apple actually did send alerts to users on April 30, 2025, warning them they might be targeted by "mercenary spyware attacks." Two of the users Apple alerted were Ciro Pellegrino, an Italian journalist for Fanpage, and Eva Vlaardingerbroek, a Dutch right-wing activist. An excerpt of the alert reads, *"Apple detected that you are being targeted by a mercenary spyware attack that is trying to remotely compromise the iPhone associated with your Apple ID -xxx-…This attack is likely targeting you specifically because of who you are or what you do. Although it's never possible to achieve absolute certainty when detecting such attacks, Apple has high confidence in this warning — please take it seriously."*

While we know the shingles vaccine is effective at preventing shingles, evidence is mounting that it might also reduce the risk of dementia. **Yes, a vaccination to prevent shingles may lessen your risk of dementia**, according to an article from Harvard Health. A vaccine to prevent shingles is recommended for adults ages 50 and older, and for people 19 and older who have an impaired immune system. Some (though not all) studies have found that having shingles increases your risk of dementia in the future. And that's led researchers to explore the possibility that preventing shingles through vaccination might reduce dementia risk. Several studies suggest this is true.

Converting a .pdf to a .docx and back again may seem like a quick and easy thing you can do online for free — but that doesn't mean it's safe. **A new notice from the FBI Denver Field Office warns that some online document converters are also loading malware onto unsuspecting users' computers, giving bad actors access to your device and your data**, according to an article from Lifehacker. The tools may also scrape files submitted for conversion for sensitive information, such as Social Security numbers, birthdates, email addresses, passwords or tokens to bypass multi-factor authentication, banking information, and cryptocurrency seed phrases and wallet addresses. This scheme may be easy to miss, as the malicious file converters will do what they advertise, such as converting a .docx to a .pdf or joining multiple files into one. However, the file you download may contain hidden ransomware, adware, or riskware that exposes your computer to attackers. You may also be prompted to download a conversion tool (that is actually malware) to your device or install a malicious browser extension. According to a Malwarebytes Labs report on the scam, the following domains have been found to contain malware:

Imageconvertors[.]com (Phishing),
convertitoremp3[.]it (Riskware),
convertisseurs-pdf[.]com (Riskware),
convertscloud[.]com (Phishing),
convertix-api[.]xyz (Trojan),
convertallfiles[.]com (Adware),
freejpgtopdfconverter[.]com (Riskware),
primeconvertapp[.]com (Riskware),
9convert[.]com (Riskware),
and Convertpro[.]org (Riskware).

While these are known scams, that doesn't mean there aren't other free, malware-containing file converters out there waiting to infect your device. The best thing you can do is avoid these tools entirely and utilize trusted software instead. Fortunately, under Linux, there are other, better ways to perform file conversions with bona fide Linux tools.

Bing Image Creator

New research suggests that octopuses and humans may share an ancient evolutionary connection that helps explain the remarkable intelligence of cephalopods, says an article from Daily Galaxy. According to findings discussed by New Scientist, both species could trace their cognitive complexity back to a common ancestor that lived around 518 million years ago. The key to this complexity lies in microRNAs (miRNAs) — small, regulatory molecules that control how genes are expressed. A study led by Nikolaus Rajewsky at the Max Delbrück Centre for Molecular Medicine revealed that soft-bodied cephalopods like octopuses experienced a “massive expansion of the miRNA gene repertoire.” This significant increase appears to be a major driver behind the evolution of their advanced brains, allowing for the creation of more diverse neuron types.

If you receive an email about your Social Security statement, proceed with caution, states an article from Lifehacker. According to a new report from Malwarebytes Labs, hackers are impersonating the Social Security Administration (SSA) to trick people into installing a remote access tool and handing over full control of their devices. The SSA is no stranger to phishing scams — the Office of the Inspector General put out an alert last month warning the public of fraudulent emails purporting to include Social Security statements that in reality led to fake websites.

OpenAI is reversing a controversial shift toward becoming a fully for-profit company, saying its founding nonprofit will remain in charge of the AI powerhouse behind ChatGPT, according to an article from TechRepublic. The announcement follows months of mounting criticism about OpenAI’s possible for-profit pivot from former employees, AI experts, and co-founder Elon Musk. In a statement, board chair Bret Taylor reaffirmed the nonprofit’s authority: “OpenAI was founded as a nonprofit, and is today overseen and controlled by that nonprofit. Going forward, it will continue to be overseen and controlled by that nonprofit.”

ICYMI: China-linked Cyber Espionage Group Compromise Multiple Organizations In SE Asia

Image by BearyBoo from Pixabay

Scammers can make good money by selling you something you can actually get for free — like government services. **The Federal Trade Commission is alerting consumers to fraudulent websites that are claiming to be associated with the IRS and charging up to $300 to file paperwork for obtaining an Employer Identification Number (EIN)**, according to an article from Lifehacker. The EIN application is available for free on the real IRS website and requires just a few minutes to complete. An EIN, which is a corporate identifier for filing taxes, is required for anyone opening a business, estate, or nonprofit as well as those with household employees (such as a family hiring a nanny).

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.

According to an article from TechCrunch, **Microsoft employees aren't allowed to use DeepSeek due to data security and propaganda concerns**, Microsoft Vice Chairman and President Brad Smith said in a Senate hearing on May 8, 2025. "At Microsoft we don't allow our employees to use the DeepSeek app," Smith said, referring to DeepSeek's application service (which is available on both desktop and mobile). Smith said Microsoft hasn't put DeepSeek in its app store over those concerns, either. Although lots of organizations and even countries have imposed restrictions on DeepSeek, this is the first time Microsoft has gone public about such a ban.

Image by Mohamed Hassan from Pixabay

Email-based attacks continued to cost enterprises big bucks in 2024, according to new cyber-insurance claims data, according to an article from Dark Reading. Cyber-insurance carrier Coalition published its "2025 Cyber Claims Report" on May 7, showing that business email compromise (BEC) attacks and fund transfer fraud (FTF) accounted for 60% of all the company's claims last year. BEC attacks were particularly problematic for customers, according to Coalition; claims severity for such threats increased 23%, with incident's costing organizations, on average, $35,000. That dollar figure is a far cry from the average loss for ransomware attacks in 2024, which Coalition said was $292,000. However, the claims report, which features data from customers in the US, the UK, Canada, and Australia, offered some encouraging data points, including a 7% drop in ransomware claims severity and a 3% decline in claims frequency.

Android's May 2025 security update includes patches for an exploited vulnerability in the FreeType open source rendering engine, according to an article from Security Week. Google on Monday started rolling out a fresh security update for Android phones, with fixes for roughly 50 vulnerabilities, including a bug exploited in the wild. Resolved as part of the update's first part, which arrives on devices as the 2025-05-01 security patch level, the exploited flaw is tracked as CVE-2025-27363 (CVSS score of 8.1) and impacts the FreeType software development library. The issue is described as an out-of-bounds write in the open source rendering engine's versions up to and including 2.13.0 that could lead to arbitrary code execution. "There are indications that CVE-2025-27363 may be under limited, targeted exploitation," Google notes in Android's May

2025 security bulletin. The internet giant rolled out patches for the bug roughly two months after Facebook parent company Meta warned that it had been exploited as a zero-day, urging organizations to update to FreeType version 2.13.3 or later.

Elementl Power Inc. is a "technology agnostic" nuclear project developer looking to bring more than 10 gigawatts of new nuclear power on line in the United States by 2035, and Google wants to see more baseload nuclear power supplying its data centers, according to an article from NuclearNewswire. The two companies announced May 7 that they have signed a strategic agreement to "pre-position" three project sites for advanced nuclear energy. Google plans to provide "early-stage capital" to help Elementl prepare three potential U.S. nuclear reactor projects, each with "at least 600 MW" of capacity. While the locations have not been announced, they are likely to be where Google wants more baseload power for data centers. The agreement gives Google the option for commercial off-take once the projects are complete, as part of "continued work to source 24/7 baseload energy to support our operations and strengthen power grids," Google said.

Google has agreed to pay the U.S. state of Texas nearly $1.4 billion to settle two lawsuits that accused the company of tracking users' personal location and maintaining their facial recognition data without consent, according to an article from The Hacker News. The $1.375 billion payment dwarfs the fines the tech giant has paid to settle similar lawsuits brought by other U.S. states. In November 2022, it paid $391 million to a group of 40 states. In January 2023, it paid $29.5 million to Indiana and Washington. Later that September, it forked out another $93 million to settle with California. The case, originally filed in 2022, related to unlawful tracking and collection of user data, regarding geolocation, incognito searches, and biometric data, tracking users' whereabouts even when the Location History setting was disabled and collecting the biometric data without informed consent.

The FBI is warning owners of some internet routers their devices could leave them vulnerable to cyber attacks, according to an article from AL.com. The new bulletin from the FBI's Cyber Division said some old routers – known as End-of-Life routers or EOLs – have known vulnerabilities that can make them easy to infiltrate and install malware. Then, the routers can be used to "launch coordinated attacks or sell access to the devices as proxy services," the bulletin noted. Routers that were made years ago are not supported by vendors with software updates or patches to fix known vulnerabilities. Scammers, aware of this lack of protection, can hijack the routers and then sell off the access.

Three Russian nationals as well as a Kazakhstani citizen were arrested and charged with conspiracy and other cybercrimes, according to a recently unsealed domain seizure warrant and indictment, says an article from Dark Reading. Alexey Viktorovich Chertkov, Kirill Vladimirovich Morozov, Aleksandr Aleksandrovich Shishkin, and Dmitriy Rubtsov were charged with conspiracy and damage to protected computers for their involvement in botnet services known as Anyproxy and 5socks. Additionally, Chertkov and Rubtsov were charged with false registration of a domain name after they allegedly falsely identified themselves when they registered and used the domains to commit their crimes. According to the indictment, a botnet was created by installing malware on older-model wireless Internet routers without the victims' knowledge, allowing the routers to be reconfigured and granting the threat actor unauthorized access to third parties as well as "making the routers available for sale as proxy servers on the Anyproxy.net and 5socks.net websites." The threat actor was able to do this to routers globally, including in the United States. In fact, the website domains for both botnet domains were managed by a company based in Virginia, while hosted on computer services worldwide.

Image by Patrick Fischer from Pixabay

NASA's Webb space telescope has captured haunting new views of Jupiter's auroral display, revealing the bright light show in exquisite, never-before-seen details, according to an article from Gizmodo. Using the telescope's most recent observations of the gas giant, scientists uncovered a curious discrepancy between how Jupiter's auroras appear to Webb versus Hubble. Webb's NIRCam (Near-Infrared Camera) zoomed into Jupiter's poles to capture the planet's fast-varying auroral features, which are 100 times brighter than the ones seen on Earth. The team plans on carrying out follow-up observations of Jupiter's auroras using Webb and comparing them to data collected by the ongoing Juno mission. The spacecraft has been orbiting the gas giant since 2016, capturing Jupiter and its moons in exquisite detail. Webb previously captured images of Jupiter's glowing auroras at its north and south poles, providing scientists with a new perspective of the planet's light display in infrared wavelengths.

A new study inspired by a student's question has found something surprising about human fingers, and how they wrinkle after being placed in water, according to an article from IFL Science. When you put your fingers into water for a reasonable amount of time, you probably notice that they begin to go wrinkly, or "prune-like" in appearance. While you may reasonably guess that this is because of your fingers becoming waterlogged, this is not the case. In 1935, doctors noticed that patients with damage to the median nerve running down the arm to the hand do not get wrinkles on their fingers after their hands are submerged in water, suggesting that the phenomenon is controlled by our nervous systems. If it were a case of skin being waterlogged, water-induced prune fingers would not be absent in patients with nerve damage.

People who live near golf courses may be 126% more likely to develop Parkinson's disease, due to the pesticides used on the expansive lawns, according to an article from People. Researchers looked at Parkinson's disease cases diagnosed near golf course locations and residential areas that share water sources with the courses, for a study published in the Journal of the American Medical Association, using data from 27 counties in Wisconsin and Minnesota. Parkinson's disease is a degenerative nervous system disorder that impacts movement. Initial symptoms are tremors or other involuntary movements. As Mayo Clinic explains, there is no cure, but surgery and treatments can help symptoms.

Image by Pete Linforth from Pixabay

Ransomware attacks, which restrict data access and encrypt information unless ransom payments are made, increasingly threaten health care operations, according to a study published on JAMA Network. In February 2024, a ransomware attack on Change Healthcare compromised the protected health information (PHI) of 100 million individuals, disrupted care delivery nationwide, and incurred $2.4 billion in response costs. Although hacking or information technology (IT) incidents became the leading cause of health care data breaches in 2017, the proportion involving ransomware remains unclear. Prior research identified 376 ransomware attacks on health care delivery organizations from 2016 to 2021, but health plans and clearinghouses have also been victims. This study analyzes ransomware attacks across all Health Insurance Portability and Accountability Act (HIPAA)–covered entities from 2010 to 2024 and examines their contribution to PHI data breaches.

Cybernews researchers have uncovered a massive data leak, which was traced back to HireClick, a recruitment platform for small to mid-sized businesses, according to an article from Cybernews. The platform helps businesses manage job listings, candidate applications, and the hiring process. The company left over 5.7 million files wide open for anyone on the internet thanks to a misconfiguration of Amazon AWS S3 storage bucket. The leaked files exposed sensitive and private information of job seekers, mainly resumes.

Data breaches are most often the work of external bad actors, but sometimes the call comes from inside the house. **Cryptocurrency exchange Coinbase has disclosed that hackers paid off support agents — both employees and contractors located outside the U.S. — who had access to company systems to provide customer data and then demanded a $20 million ransom not to leak the information**, according to an article from Lifehacker. Coinbase was notified of the ransom demand on May 11, just a few days before reporting the incident to the Securities and Exchange Commission (SEC). The company has said the staff involved were fired and reported to law enforcement when their unauthorized access was detected, but they were still able to provide information to attackers.

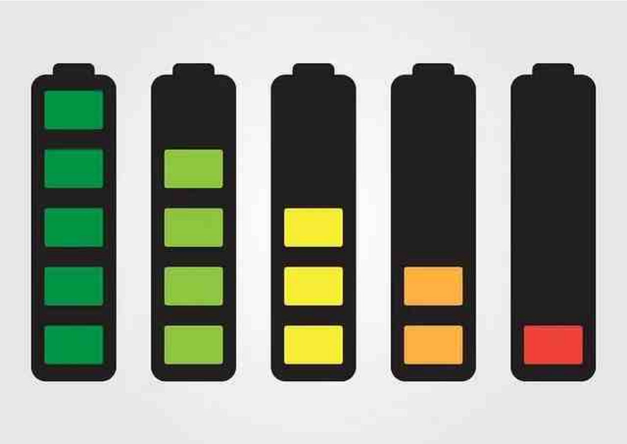


Image by Денис Марчук from Pixabay

Following an advisory from the FAA, TSA says it is now banning passengers from storing portable chargers and power banks that use lithium batteries in their checked bags, according to an article from Yahoo! News. Any lithium-ion and lithium-metal batteries, including power banks and portable charging devices, now must be stored in carry-on luggage only. “When a carry-on bag is checked at the gate or at planeside, all spare lithium batteries and power banks must be removed from the bag and kept with the passenger in the aircraft cabin. The battery terminals must be protected from short circuit,” the FAA stated. “This covers spare lithium metal and spare rechargeable lithium-ion batteries for personal electronics such as cameras, cell phones, laptop computers, tablets, watches, calculators, etc. This also includes external battery chargers (portable rechargers) containing a lithium-ion battery.”

There's a lot of advice out there for proper password management: Each of your passwords should be strong and unique; use a secure manager to store your passwords; use two-factor authentication (2FA) to add an extra layer of security to your accounts. But there's another piece of advice that is held in the same regard as the others: **Change your passwords often** — perhaps once every three months. This habit is so emphasized, many companies and organizations will make you change your passwords multiple times a year in the name of security. **The thing is, in all likelihood, this isn't actually doing anything to help your security**, according to an article from Lifehacker. This idea that changing your passwords multiple times a year is a cornerstone of your security, might be engrained in some of you. After all, it's not new advice. As PCMag examined, the practice goes back a long time: When security experts write about passwords, they often write about changing passwords, too. It's just the way the advice has been presented. But that's likely because it's anticipating and responding to bad security habits.

In a shocking revelation for the cybersecurity community, it has been discovered that Procolored, a popular printer manufacturer, unknowingly distributed malware-infected printer drivers for over six months, according to an article from Freedium. These malicious packages were bundled with software for multiple printer models and included Remote Access Trojans (RATs) and a cryptocurrency-stealing malware called SnipVex. The malware fiasco came to light when Serial Hobbyism, a YouTube tech creator, attempted to install drivers for his $7,000 Procolored UV printer. His security software immediately flagged the files as malicious, citing the **Floxif USB worm** — a red flag that couldn't be ignored.

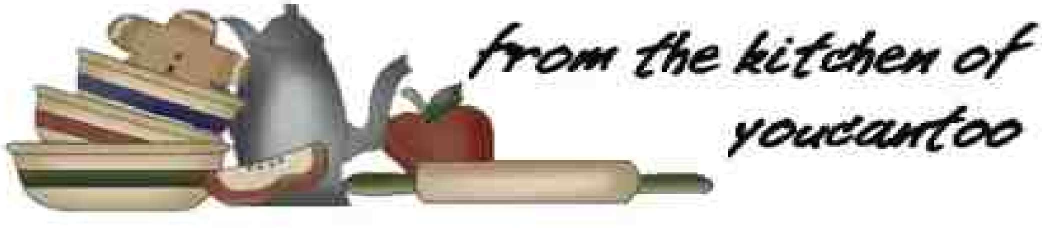
23andMe's new buyer, paying $256 million for the company's assets, is Regeneron, according to an article from Lifehacker. Regeneron is a biotech company perhaps best known for developing an antibody treatment for COVID early in the pandemic. That treatment never made it all the way to market, but the company does market other antibody- and protein-based treatments for conditions like Ebola virus, genetic disorders, and cancers. Regeneron's website states that they "are shaping the next frontier of medicine with data-powered insights from the Regeneron Genetics Center® and pioneering genetic medicine platforms, enabling us to identify innovative targets and complementary approaches to potentially treat or cure diseases." That explains why they're interested in 23andMe, since it provides a trove of genetic data. Many 23andMe users had also signed up to provide more of their personal medical information for research purposes (this was a separate thing that you would have had to opt in to provide). Regeneron says they plan to "continue all consumer genome services uninterrupted," rather than shut down the company. Lemonaid health, also owned by 23andMe, is not included in the sale. Importantly, Regeneron says they will respect the company's privacy policy ("and applicable laws") and the 23andMe press release also says that Regeneron will not be making any changes to the privacy policy.

If you get a text or voice message from someone claiming to be a U.S. government official, they probably aren't who they say they are, according to an article from Lifehacker. The FBI is warning the public about an ongoing campaign in which scammers are using AI-generated voice messages to impersonate senior government staff in an attempt to gain access to personal accounts and, by extension, sensitive information or money. Many of those targeted have been other current and former government officials—both federal and state—and their contacts, but that doesn't mean this scam or something like it won't land in your inbox or on your phone sooner or later.

A trio of phone surveillance apps, which was caught spying on millions of people's phones earlier this year, has gone offline, according to an article from TechCrunch. Cocospy, Spyic, and Spyzie were three near-identical but differently branded stalkerware apps that allowed the person planting one of the apps on a target's phone access to their personal data — including their messages, photos, call logs, and real-time location data — usually without that person's knowledge. Stalkerware apps, like Cocospy and its clones, are designed to stay hidden from device home screens, making the apps difficult to detect by their victims but all the while making the phone's contents continually available to the person who planted the app.

Security researcher Jeremiah Fowler found a public online database housing over 180 million records (184,162,718 to be exact) which amounted to more than 47GB of data, according to an article from Lifehacker. There were no indications about who owned the data or who placed it there, which Fowler says is atypical for these types of online databases. Fowler saw emails, usernames, passwords, and URLs linking to the sites where those credentials belonged. These accounts included major platforms like Microsoft, Facebook, Instagram, Snapchat, Roblox, Apple, Discord, Nintendo, Spotify, Twitter, WordPress, Yahoo, and Amazon, as well as bank and financial accounts, health companies, and government accounts from at least 29 countries. That includes the U.S., Australia, Canada, China, India, Israel, New Zealand, Saudi Arabia, and the UK.

PCLinuxOS Recipe Corner



Sausage, Egg, & Cheese Breakfast Roll-Ups

Makes: 4

INGREDIENTS:

1 lb breakfast sausage
6 large eggs
1/2 cup shredded cheddar cheese
1/4 cup milk
1/2 teaspoon salt
1/4 teaspoon black pepper
4 large flour tortillas

DIRECTIONS:

Brown the sausage in a large skillet over medium-high heat. Once it's browned, remove the sausage with a slotted spoon to a plate covered with paper towels to drain. Discard any remaining fat out of the pan, and wipe clean with a paper towel. Return pan to the stove top to cook eggs.

In a large bowl combine 6 eggs, 1/4 cup milk, and salt and pepper to taste. Whisk till the egg mixture is an even light yellow color. Pour into the HOT skillet.

Allow the eggs to cook for a minute before gently pulling the eggs from the outer edges towards the center with a flat spatula. Allow to cook for another minute, then pull in again. Repeat this process until the eggs are fully cooked. Should be light and fluffy.

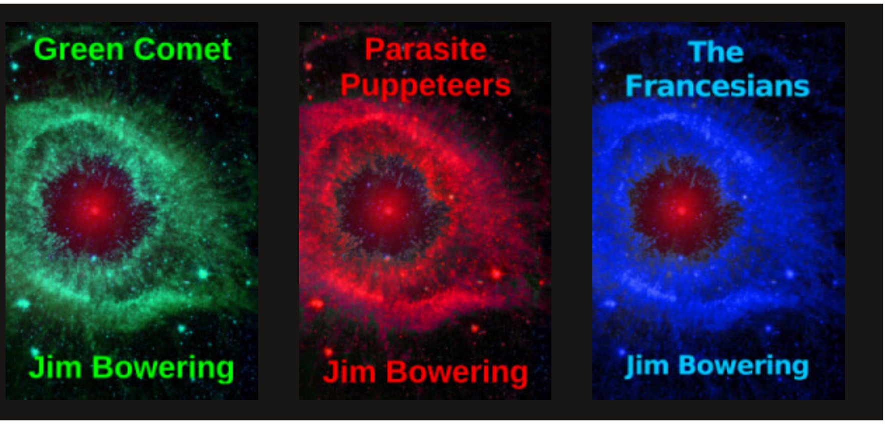
Heat oven to 375 degrees F.

Place the sausage and egg mixture in the center of a flour tortilla, add a tablespoon of cheese and then roll up. Place seam side down on a baking sheet. Repeat for the remaining tortillas.

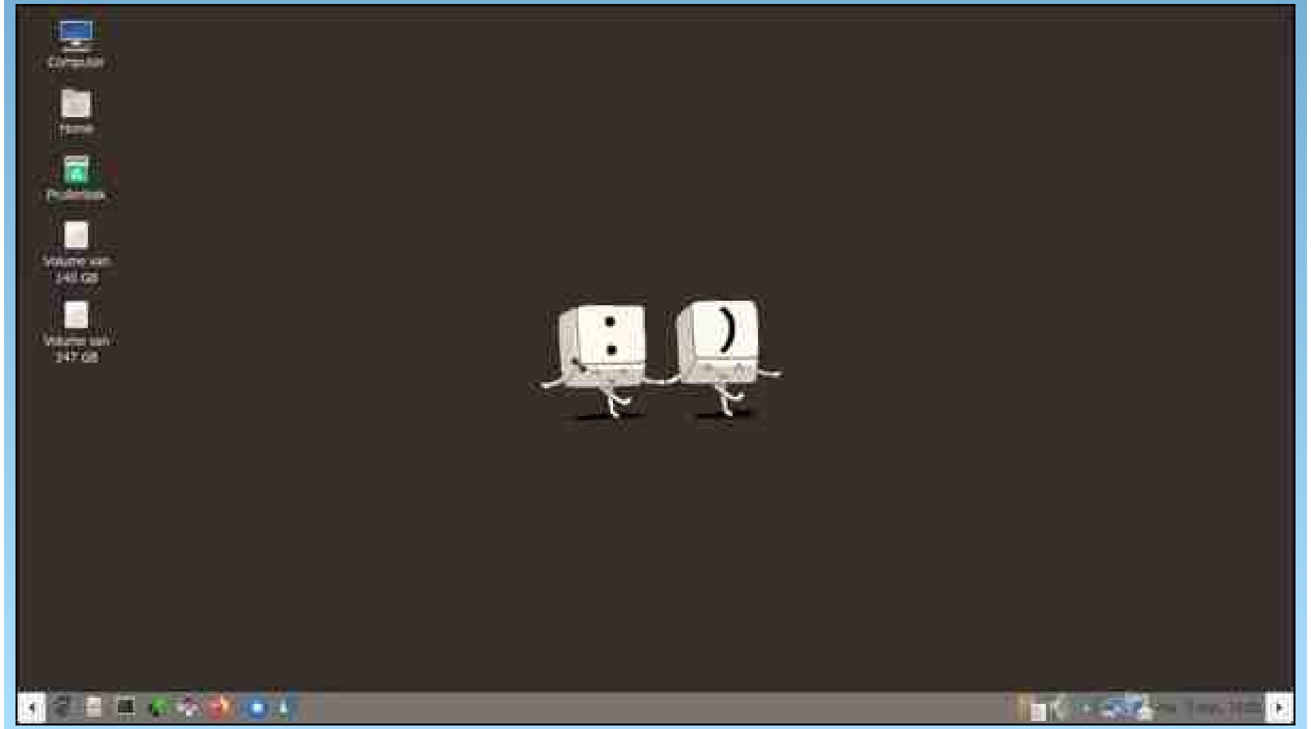
Bake for 15 minutes, then flip and bake for an additional 10 minutes. Let cool slightly and enjoy.

NUTRITION:

Calories: 368 Carbs: 16g Sodium: 665mg
Fiber: 1g Protein: 20g



Screenshot Showcase



Posted by mutse, May 5, 2025, running Mate.

Online Tracking Is Out Of Control — Privacy Badger Can Help You Fight Back

by Lena Cohen
Electronic Frontier Foundation

Every time you browse the web, you're being tracked. Most websites contain invisible tracking code that allows companies to collect and monetize data about your online activity. Many of those companies are data brokers, who sell your sensitive information to anyone willing to pay. That’s why EFF created Privacy Badger, a free, open-source browser extension used by millions to fight corporate surveillance and take back control of their data.

Since we first released Privacy Badger in 2014, online tracking has only gotten more invasive, and Privacy Badger has evolved to keep up. Whether this is your first time using it or you’ve had it installed since day one, here’s a primer on how Privacy Badger protects you.

Online Tracking Isn't Just Creepy—It’s Dangerous

The rampant data collection, sharing, and selling fueled by online tracking has serious consequences. Fraudsters purchase data to identify elderly people susceptible to scams. Government agencies and law enforcement purchase people’s location data and web browsing records without a warrant. Data brokers help predatory companies target people in financial distress. And surveillance companies repackage data into government spy tools.

Once your data enters the data broker ecosystem, it’s nearly impossible to know who buys it and what they’re doing with it. Privacy Badger blocks online tracking to prevent your browsing data from being used against you.

Privacy Badger Disrupts Surveillance Business Models

Online tracking is pervasive because it’s profitable. Tech companies earn enormous profits by targeting ads based on your online activity—a practice called “online behavioral advertising.” In fact, Big Tech giants like Google, Meta, and Amazon are among the top companies tracking you across the web. By automatically blocking their trackers, Privacy Badger makes it harder for Big Tech companies to profit from your personal information.

Online behavioral advertising has made surveillance the business model of the internet. Companies are incentivized to collect as much of our data as possible, then share it widely through ad networks with no oversight. This not only exposes our sensitive information to bad actors, but also fuels government surveillance. Ending surveillance-based advertising is essential for building a safer, more private web.

While strong federal privacy legislation is the ideal solution — and one that we continue to advocate for — Privacy Badger gives you a way to take action today.

Privacy Badger fights for a better web by incentivizing companies to respect your privacy. Privacy Badger sends the Global Privacy Control and Do Not Track signals to tell companies not to track you or share your data. If they ignore these signals, Privacy Badger will block them, whether they are advertisers or trackers of other kinds. By withholding your browsing data from advertisers, data brokers, and Big Tech companies, you can help make online surveillance less profitable.

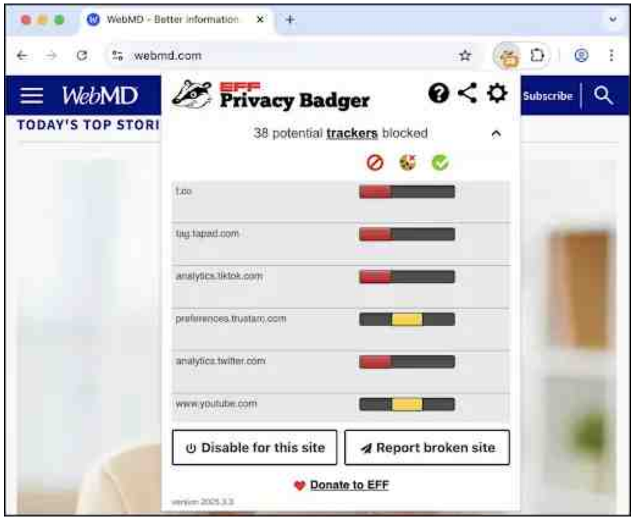
How Privacy Badger Protects You From Online Tracking

Whether you're looking to protect your sensitive information from data brokers or simply don't want Big Tech monetizing your data, Privacy Badger is here to help.

Over the past decade, Privacy Badger has evolved to fight many different methods of online tracking. Here are some of the ways that Privacy Badger protects your data:

- **Blocks Third-Party Trackers and Cookies**: Privacy Badger stops tracking code from loading on sites that you visit. That prevents companies from collecting data about your online activity on sites that they don't own.
- **Sends the GPC Signal to Opt Out of Data Sharing**: Privacy Badger sends the Global Privacy Control (GPC) signal to opt out of websites selling or sharing your personal information. This signal is legally binding in some states, including California, Colorado, and Connecticut.
- **Stops Social Media Companies From Tracking You Through Embedded Content**: Privacy Badger replaces page elements that track you but are potentially useful (like embedded tweets) with click-to-activate placeholders. Social media buttons, comments sections, and video players can send your data to other companies, even if you don't click on them.
- **Blocks Link Tracking on Google and Facebook**: Privacy Badger blocks Google and Facebook's attempts to follow you whenever you click a link on their websites. Google not only tracks the links you visit from Google Search, but also the links you click on platforms that feel more private, like Google Docs and Gmail.
- **Blocks Invasive "Fingerprinting" Trackers**: Privacy Badger blocks trackers that try to identify you based on your browser's unique characteristics, a particularly problematic form of tracking called "fingerprinting."
- **Automatically learns to block new trackers**: Our Badger Swarm research project continuously discovers new trackers for Privacy Badger to block. Trackers are identified based on their behavior, not just human-curated blocklists.
- **Disables Harmful Chrome Settings**: Automatically disables Google Chrome settings that are bad for your privacy.
- **Easy to Disable on Individual Sites While Maintaining Protections Everywhere Else**: If blocking harmful trackers ends up breaking something on a website, you can disable Privacy Badger for that specific site while maintaining privacy protections everywhere else.

All of these privacy protections work automatically when you install Privacy Badger — there's no setup required! And it turns out that when Privacy Badger blocks tracking, you'll also see fewer ads and your pages will load faster.



38 potential trackers blocked

t.co
tag.tapad.com
analytics.tiktok.com
preferences.trustarc.com
analytics.twitter.com
www.youtube.com

You can always check to see what Privacy Badger has done on the site you're visiting by clicking on Privacy Badger's icon in your browser toolbar.

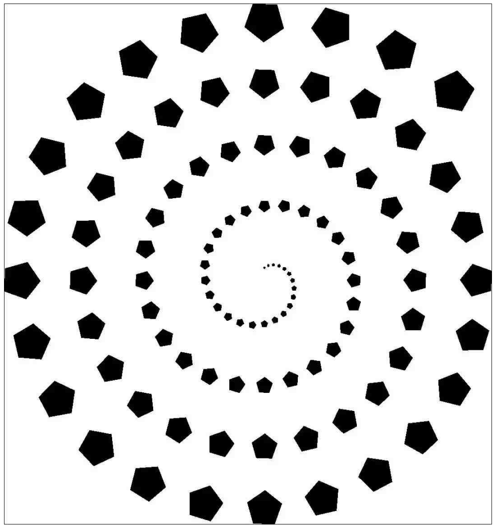
Fight Corporate Surveillance by Spreading the Word About Privacy Badger

Privacy is a team sport. The more people who withhold their data from data brokers and Big Tech companies, the less profitable online surveillance becomes. If you haven't already, visit privacybadger.org to install Privacy Badger on your web browser. And if you like Privacy Badger, tell your friends about how they can join us in fighting for a better web!

Inkscape Tutorial: A Tiled Clone Trick

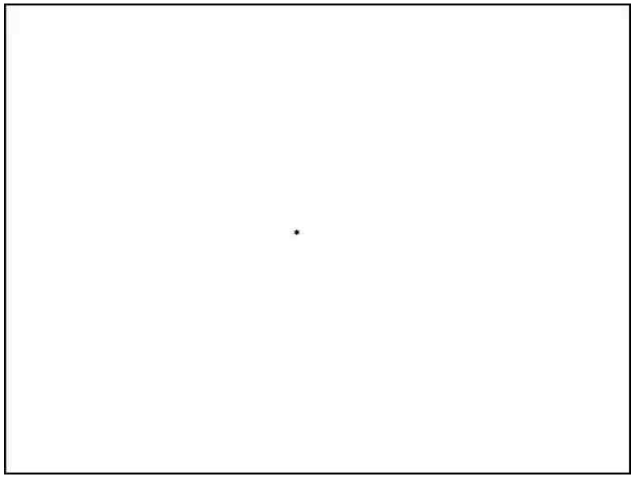
by Meemaw

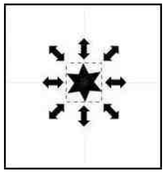
I'm always looking for new things to make with Inkscape, and I found a video from Logos By Nick that I hadn't seen before. It outlines a trick you can do with tiled clones, which makes a spiral design from a figure you choose. It's fairly easy and can be edited as well.



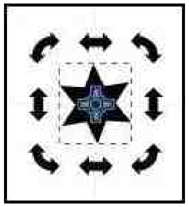
Opening Inkscape, start a new project. Make the canvas big, maybe 1,800 × 1,200 px. Depending on your starting object, the finished product may be bigger than the page.

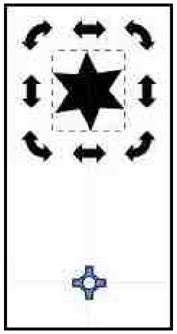
Draw the object you want to use. I did this 3 times, and used a triangle, a pentagon and a 5-pointed star. This time I'll use a 6-pointed star. Change the size so it's very small, because the tiled clones tool will increase the size as it makes the spiral. You can see how big it is on the page and what I drew.





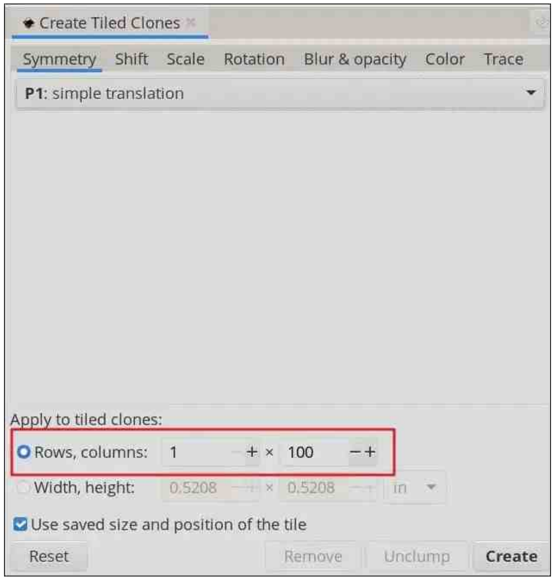
You can eventually use any color you want, but let's use black fill and no stroke. Select the star (or whatever you used) as shown above. Click it once again to show the rotation handles. Holding down the **<CTRL>** key, drag the center rotation handle down under the star.





Keeping your star selected, click **Edit > Clone > Create Tiled Clones…** If you have used this tool at all, the first thing you should do is click on Reset to reset the settings back to the defaults. Then, use the settings below (under the indicated tab).

Symmetry



P1: simple translation

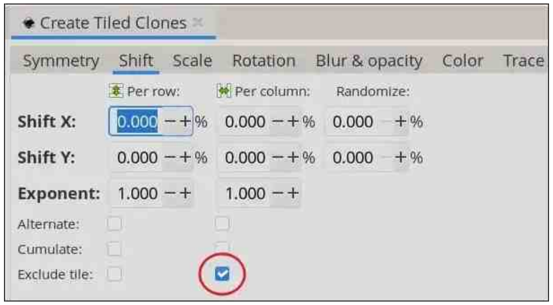
Apply to tiled clones:

● Rows, columns: 1 × 100

○ Width, height: 0.5208 × 0.5208 in

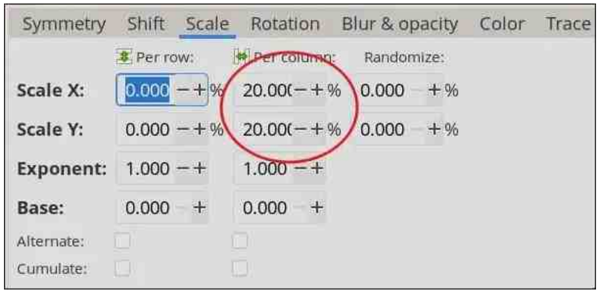
☑ Use saved size and position of the tile

Shift



	Per row:	Per column:	Randomize:
Shift X:	0.000 %	0.000 %	0.000 %
Shift Y:	0.000 %	0.000 %	0.000 %
Exponent:	1.000	1.000	
Alternate:	□	□	
Cumulate:	□	□	
Exclude tile:	□	☑	

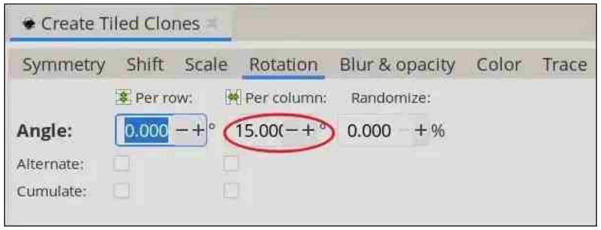
Scale



Symmetry | Shift | Scale | Rotation | Blur & opacity | Color | Trace

	Per row:	Per column:	Randomize:
Scale X:	0.000 %	20.00(%	0.000 %
Scale Y:	0.000 %	20.00(%	0.000 %
Exponent:	1.000	1.000	
Base:	0.000	0.000	
Alternate:	☐	☐	
Cumulate:	☐	☐	

Rotation

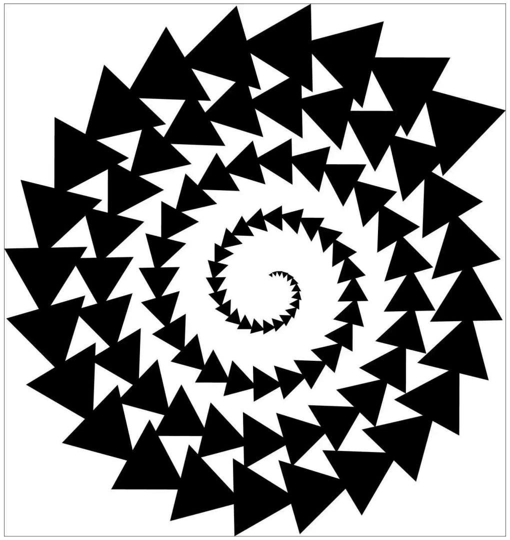


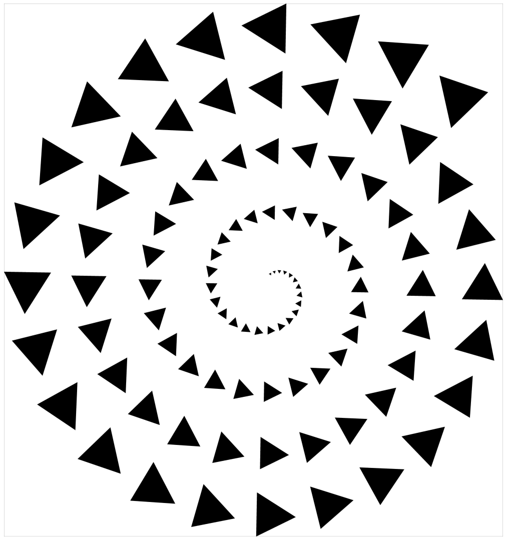
Create Tiled Clones

Symmetry | Shift | Scale | Rotation | Blur & opacity | Color | Trace

	Per row:	Per column:	Randomize:
Angle:	0.000 °	15.00(°	0.000 %
Alternate:	☐	☐	
Cumulate:	☐	☐	

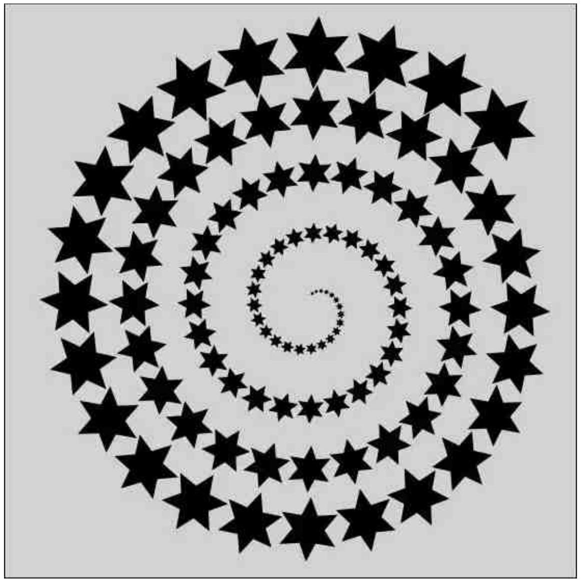
Click on **Create**. Depending on how far down you dragged the rotation handle, you might get something you like, or something you don't. Earlier, I got these:

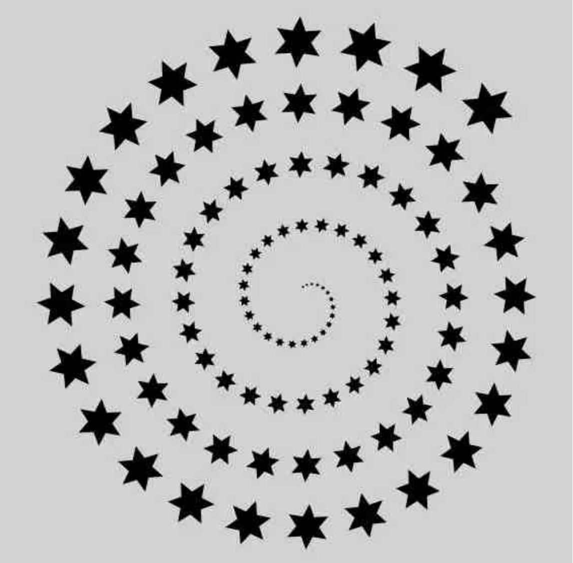




On the first example, the triangles were a bit too close together, so I pulled the center rotation handle down more, and on the second example, it looked better to me. The change is easily made by clicking **<CTRL> + Z** to undo the version you don't want, making the change to the handle, and then clicking Create again.

Another thing you can do is make changes to the spiral by manipulating the original star/triangle/whatever you used. When you clone the original, the first clone goes on top of the original, but if you send the first clone to the bottom, and manipulate the original, all the clones will change automatically. On mine, after I made the first spiral, I grabbed the original star and sized it down a bit more, and watched the spiral change.





Experiment with the settings to see what can be done. Decreasing the rotation percent sets your clones closer together, I believe. You may not like the way that looks, but it's your creation (always), and only you know what you want.

Typst Cookbook, Part Two

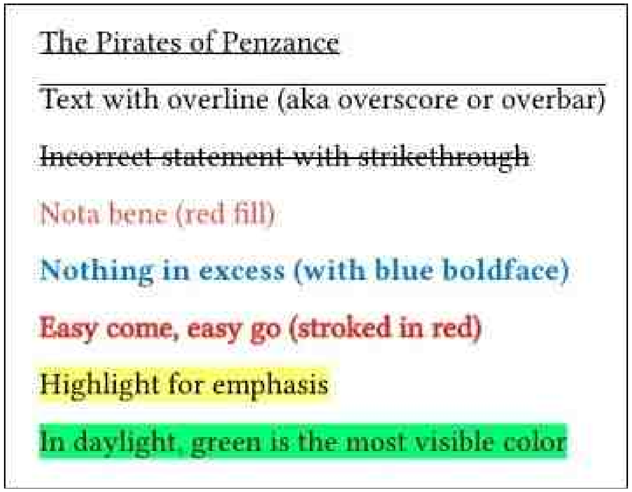
by David Pardue (kalwisti)

In my previous article, I offered some practical tips for using Typst more efficiently. This month, we will take a look at additional Typst features which should help you create more typographically complex documents.

Simple Text Formatting

Typst's `text` function can customize the appearance and layout of text in various ways. The source code below produces the output shown in the screenshot:

```
#underline[The Pirates of Penzance]

#overline[Text with overline (aka overscore or overbar)]

#strike[Incorrect statement with strikethrough]

#text(fill:red)[Nota bene (red fill)]

#text(fill:blue)[*Nothing in excess (with blue boldface)*]

#text(stroke: 0.5pt + red)[Easy come, easy go (stroked in red)]

#highlight[Highlight for emphasis]

#highlight(fill:lime)[In daylight, green is the most visible color]

// This is a comment; it won't be typeset
```



The Pirates of Penzance

Text with overline (aka overscore or overbar)

~~Incorrect statement with strikethrough~~

Nota bene (red fill)

Nothing in excess (with blue boldface)

Easy come, easy go (stroked in red)

Highlight for emphasis

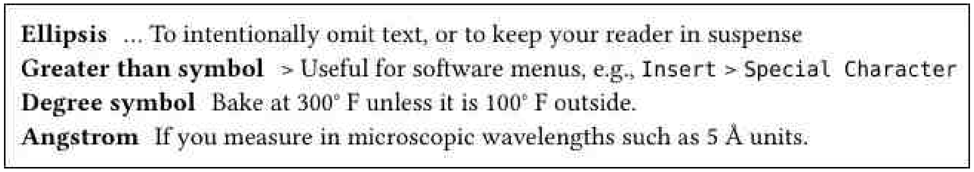
In daylight, green is the most visible color

Miscellaneous Symbols

Typst offers a comprehensive set of symbols and emojis. The general symbols below are generated with the " #sym. " prefix and might prove useful in your writing.

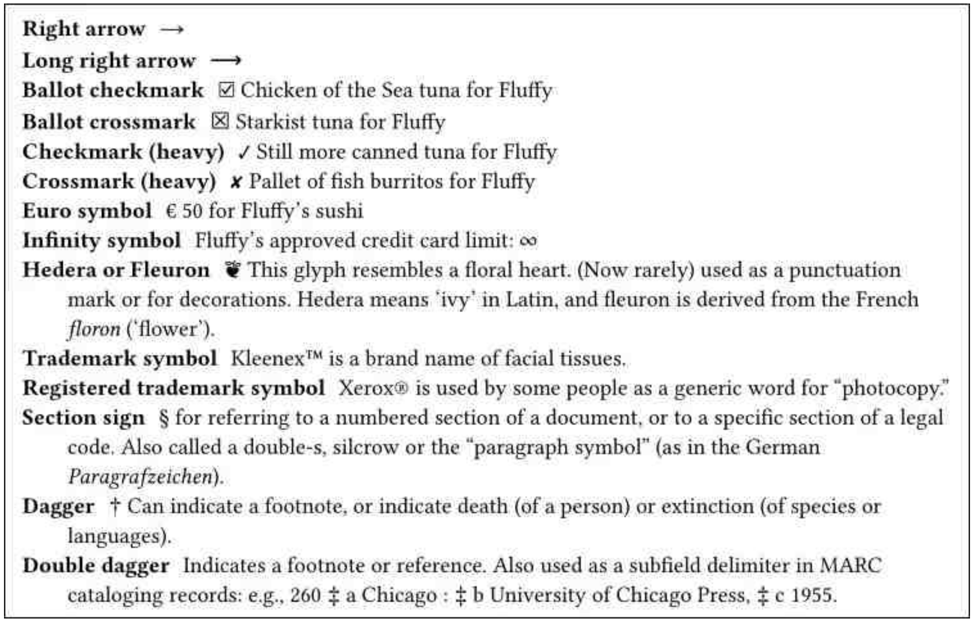
The code below produces output shown in the screenshots. (*Note*: The forward slash symbol at the beginning of each line indicates that what follows is a term. Each term ends with a colon, then the term's description comes afterward.)

```
/ Ellipsis: #sym.dots.h To intentionally omit text, or to keep your reader in suspense
/ Greater than symbol: #sym.gt Useful for software menus, e.g., `Insert` #sym.gt `Special Character`
/ Degree symbol: Bake at 300#sym.degree F unless it is 100#sym.degree F outside.
/ Angstrom: If you measure in microscopic wavelengths
such as 5 #sym.angstrom units.
```



Ellipsis … To intentionally omit text, or to keep your reader in suspense
Greater than symbol > Useful for software menus, e.g., `Insert > Special Character`
Degree symbol Bake at 300° F unless it is 100° F outside.
Angstrom If you measure in microscopic wavelengths such as 5 Å units.

```
/ Right arrow: #sym.arrow.r
/ Long right arrow: #sym.arrow.r.long
/ Ballot checkmark: #sym.ballot.check Chicken of the
Sea tuna for Fluffy
/ Ballot crossmark: #sym.ballot.cross Starkist tuna
for Fluffy
/ Checkmark (heavy): #sym.checkmark.heavy Still more
canned tuna for Fluffy
/ Crossmark (heavy): #sym.crossmark.heavy Pallet of
fish burritos for Fluffy
/ Euro symbol: #sym.euro 50 for Fluffy's sushi
/ Infinity symbol: Fluffy's approved credit card
limit: #sym.infinity
/ Hedera or Fleuron: #sym.floral This glyph resembles
a floral heart. (Now rarely) used as a punctuation
mark or for decorations. Hedera means 'ivy' in Latin,
and fleuron is derived from the French _floron_
('flower').
/ Trademark symbol: Kleenex#sym.trademark is a brand
name of facial tissues.
/ Registered trademark symbol:
Xerox#sym.trademark.registered is used by some people
as a generic word for "photocopy."
/ Section sign: #sym.section for referring to a
numbered section of a document, or to a specific
section of a legal code. Also called a double-s,
silcrow or the "paragraph symbol" (as in the German
_Paragrafzeichen_).
/ Dagger: #sym.dagger Can indicate a footnote, or
indicate death (of a person) or extinction (of species
or languages).
/ Double dagger: Indicates a footnote or reference.
Also used as a subfield delimiter in MARC cataloging
records: e.g., 260 #sym.dagger.double a Chicago :
#sym.dagger.double b University of Chicago Press,
#sym.dagger.double c 1955.
```



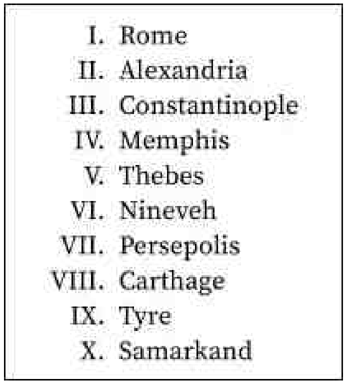
Right arrow →
Long right arrow ⟶
Ballot checkmark ☑ Chicken of the Sea tuna for Fluffy
Ballot crossmark ☒ Starkist tuna for Fluffy
Checkmark (heavy) ✔ Still more canned tuna for Fluffy
Crossmark (heavy) ✘ Pallet of fish burritos for Fluffy
Euro symbol € 50 for Fluffy's sushi
Infinity symbol Fluffy's approved credit card limit: ∞
Hedera or Fleuron ❦ This glyph resembles a floral heart. (Now rarely) used as a punctuation mark or for decorations. Hedera means 'ivy' in Latin, and fleuron is derived from the French *floron* ('flower').
Trademark symbol Kleenex™ is a brand name of facial tissues.
Registered trademark symbol Xerox® is used by some people as a generic word for "photocopy."
Section sign § for referring to a numbered section of a document, or to a specific section of a legal code. Also called a double-s, silcrow or the "paragraph symbol" (as in the German *Paragrafzeichen*).
Dagger † Can indicate a footnote, or indicate death (of a person) or extinction (of species or languages).
Double dagger Indicates a footnote or reference. Also used as a subfield delimiter in MARC cataloging records: e.g., 260 ‡ a Chicago : ‡ b University of Chicago Press, ‡ c 1955.

Enumerated List with Roman Numerals

If you need to make an outline, it is easy to switch from the default Arabic numbers to a Roman numerals style with a `#set` rule.

```
#set enum(numbering: "I.")

+ Rome
+ Alexandria
+ Constantinople
+ Memphis
+ Thebes
+ Nineveh
+ Persepolis
+ Carthage
+ Tyre
+ Samarkand
```

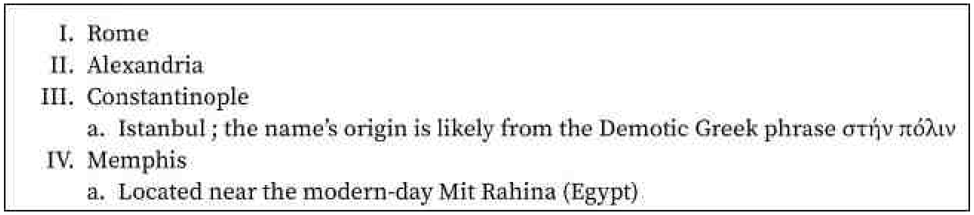
The code above produces this output:



I. Rome
II. Alexandria
III. Constantinople
IV. Memphis
V. Thebes
VI. Nineveh
VII. Persepolis
VIII. Carthage
IX. Tyre
X. Samarkand

To create a nested list, use indentation and specify a numbering pattern with multiple counting symbols (as shown in the example below):

```
#set enum(numbering: "I.a.")

+ Rome
+ Alexandria
+ Constantinople
+ Istanbul ; the name's origin is likely from the Demotic Greek phrase στήν πόλιν
+ Memphis
+ Located near the modern-day Mit Rahina (Egypt)
```



I. Rome
II. Alexandria
III. Constantinople
    a. Istanbul ; the name's origin is likely from the Demotic Greek phrase στήν πόλιν
IV. Memphis
    a. Located near the modern-day Mit Rahina (Egypt)

Raw Text / Code Blocks

If you need to embed computer code within your document, Typst provides methods to display verbatim text (with optional syntax highlighting) for several different programming languages. The Raw Text / Code function explains how to accomplish this.

For short bursts of inline code, you can use the `#box` function. The (optional) highlighting is added via a `#show` rule in conjunction with the `fill` parameter.

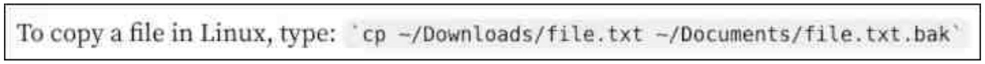
If you wish to highlight your code blocks, the Typst code below creates a pinkish fill:

```
// Display inline code in a small box
// that retains the correct baseline.
#show raw.where(block: false): box.with(
fill: luma(240),
inset: (x: 3pt, y: 0pt),
outset: (y: 3pt),
radius: 2pt,
)
```

Here is an example of brief inline code:

````
To copy a file in Linux, type: #box(``` `cp ~/Downloads/file.txt ~/Documents/file.txt.bak` ```)
````

It produces this output:

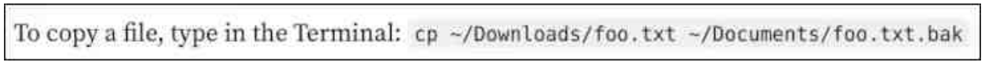


To copy a file in Linux, type: `cp ~/Downloads/file.txt ~/Documents/file.txt.bak`

The code below:

```
To copy a file, type in the Terminal: `cp ~/Downloads/foo.txt ~/Documents/foo.txt.bak`
```

Generates this output:



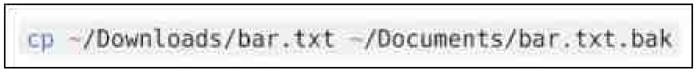
To copy a file, type in the Terminal: `cp ~/Downloads/foo.txt ~/Documents/foo.txt.bak`

With the option of **#box(```` ```language code``` ````)** you can indicate the programming/scripting language (typ [Typst], bash, py, rust, etc.)

Note: The language name is preceded by three backticks with no intervening space. This snippet of inline code

~~~~
#box(```` ```bash cp ~/Downloads/bar.txt ~/Documents/bar.txt.bak``` ````)
~~~~

Produces the output:



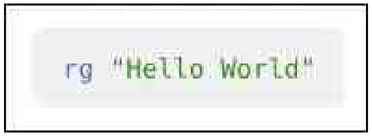
```
cp ~/Downloads/bar.txt ~/Documents/bar.txt.bak
```

If you want to display the raw text as a separate block with highlighting, insert the code below:

~~~~
// Display block code in a larger block
// with more padding.
#show raw.where(block: true): block.with(
fill:luma(240),
inset: 10pt,
radius: 4pt,
)


```bash
rg "Hello World"
```
~~~~

This produces the output shown below:



```
rg "Hello World"
```

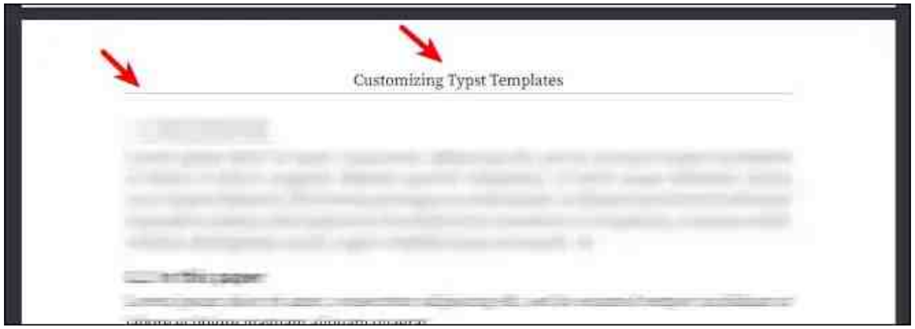
Another option for displaying code blocks is to use the codly package from Typst Universe; it allows a high degree of customization and produces attractive output. I will discuss it in a later section of my article.

Page Headers

The header parameter of Typst's page function can be configured to adjust the placement of the page header and its content. It provides control similar to the fancyhdr package in LaTeX.

Place the code below at the beginning of your Typst file. It will center the header and create a solid line that spans the width of your document. (The rect function [" #rect( ) "] in this example instructs Typst to draw/stroke the bottom edge of the rectangle, which will serve as the separating line. The text of the header will be placed inside the rectangle and centered.)

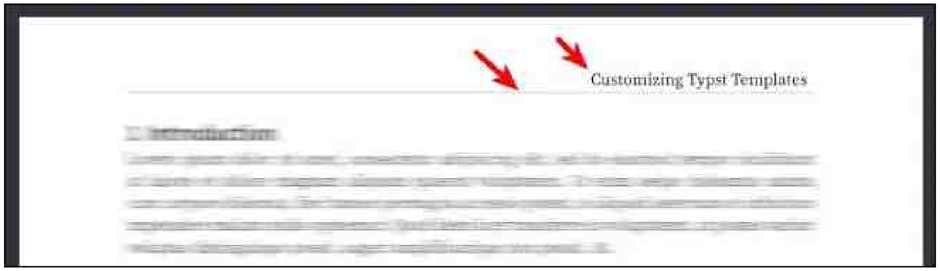
```
#set page(header:[
#rect(
stroke: (bottom:0.2pt),width: 100%,
align(center)[Customizing Typst Templates]
)
])
```



The code below will create a flush right header with a solid line beneath it:

```
#set page(header:[
#rect(
```

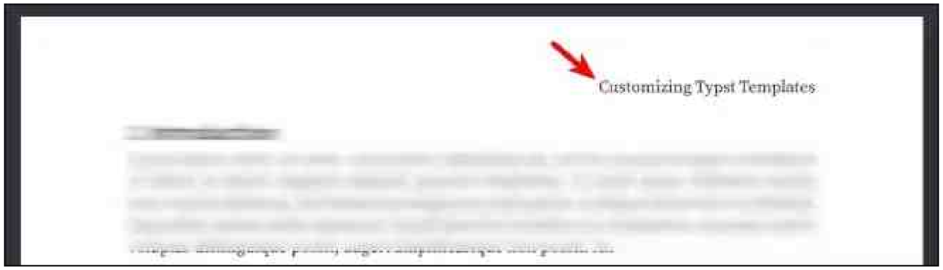
```
stroke: (bottom:0.2pt),width: 100%,
align(right)[Customizing Typst Templates]
)
])
```



Customizing Typst Templates

The code below generates a flush right header without a solid line:

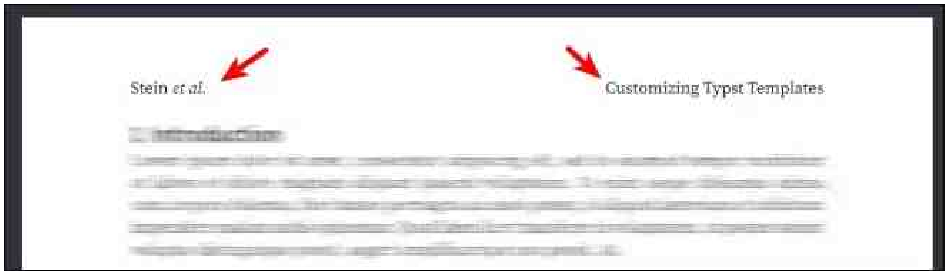
```
#set page(header: [#align(right)[Customizing Typst
Templates]])
```



Customizing Typst Templates

Finally, the code snippet below creates a header with the authors' names flush left, and the article's title flush right:

```
#set page(header: [Stein _et al._ #h(1fr) Customizing
Typst Templates])
```



Stein *et al.*

Customizing Typst Templates

Endnotes

Endnotes are not currently implemented in Typst, but they are on the development roadmap (under the "Layout" section). Typst user aarnent, however, created a skeleton that allows the use of footnotes. It works—both locally and in Typst's web app—and is customizable (if you understand Typst coding). You can access his shared Typst project for more details. His workaround enables simultaneous endnote and footnote capability, if you wish.

The History StackExchange has a lengthy discussion about publishers' use of endnotes versus footnotes. Many publishers prefer endnotes because they are cheaper (requiring less fiddling by typesetters) and easier to manage, even though they inconvenience readers by making them jump back and forth between the main text and the endnotes.

```
#let allendotes = state("endnotes", ())
#let endnote(cnt) = {
allendotes.update(x => {
x.push(cnt + parbreak())
return x
})
context super[#allendotes.get().len()]
}

#let showendnote() = context {
v(2em)
align(center, heading(level: 2)[Notes])
for (idx, cnt) in allendotes.get().enumerate() {
super[#(idx + 1)] + cnt
}
}

#show heading: it => {
if it.level == 1 {
allendotes.update(x => ())
}
it
}
```

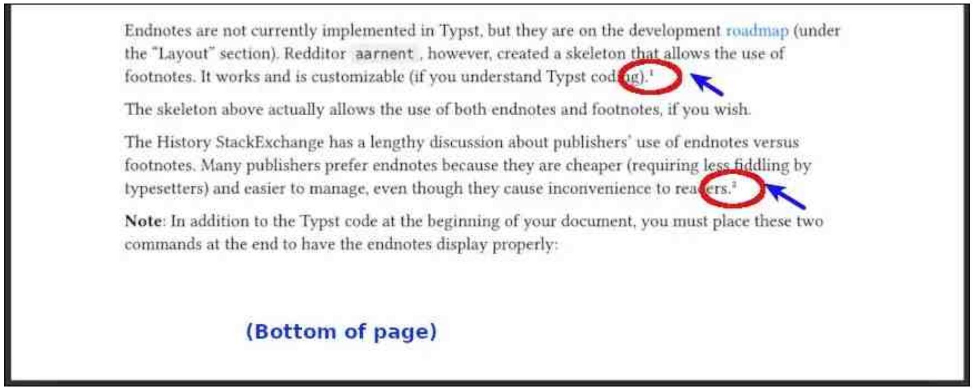
Note: Place the Typst code (above) at the beginning of your document. In addition, you must place these two commands at the end of your Typst file, so that the endnotes display properly:

```
#pagebreak()

#showendnote()
```

The `#endnote` command is called with the syntax below. (I truncated this code for two endnote commands to save space.)

```
<snip> ... understand Typst coding).#endnote[See his shared Typst project at https://typst.app/project/rnU99-7IT8dbMjGTVceOqs for more details.]

<snip> ... inconvenience to readers.#endnote[See https://tinyurl.com/3wemtjn4 for the opinionated discussion.]
```

The screenshots below show the generated Typst output:



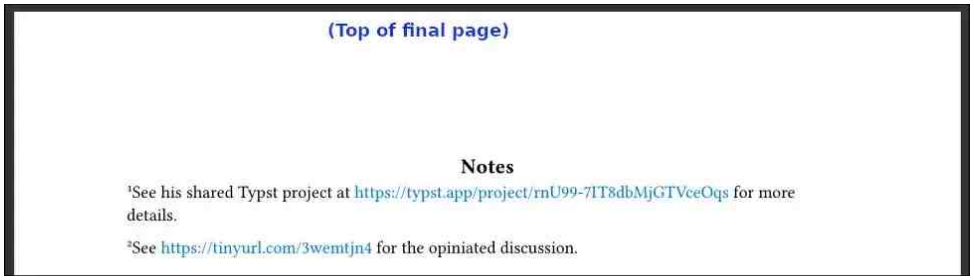
Endnotes are not currently implemented in Typst, but they are on the development roadmap (under the "Layout" section). Redditor `aarnent` , however, created a skeleton that allows the use of footnotes. It works and is customizable (if you understand Typst coding).[1]

The skeleton above actually allows the use of both endnotes and footnotes, if you wish.

The History StackExchange has a lengthy discussion about publishers' use of endnotes versus footnotes. Many publishers prefer endnotes because they are cheaper (requiring less fiddling by typesetters) and easier to manage, even though they cause inconvenience to readers.[2]

Note: In addition to the Typst code at the beginning of your document, you must place these two commands at the end to have the endnotes display properly:

(Bottom of page)



(Top of final page)

Notes

[1] See his shared Typst project at https://typst.app/project/rnU99-7IT8dbMjGTVceOqs for more details.

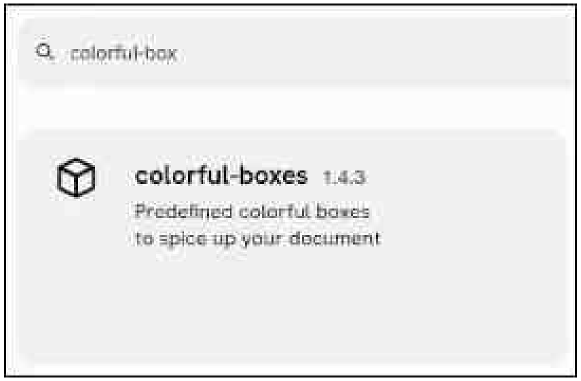
[2] See https://tinyurl.com/3wemtjn4 for the opinionated discussion.

Importing Packages from Typst Universe

Typst Universe is a collection of packages and templates to enhance Typst. I have been exploring various packages and would like to cover a few which I found useful in my writing. I hope they will benefit you as well.

(As user `sitandr` points out, we should remember that—unlike in LaTeX—Typst packages are needed only for some specialized tasks because basic formatting can be handled without them. In addition, Typst packages are much lighter/smaller and more easily installed than LaTeX packages.)

The procedure below will import a package into Typst's web app or the Typst compiler installed locally. I will use the `colorful-boxes` package as an example; however, this method works identically for the other packages that I describe. Go to Typst Universe: https://typst.app/universe. In the `Search` box, type the name of the package that you wish to import. A list of Search results will be displayed. Click on your desired package to read more information about it.

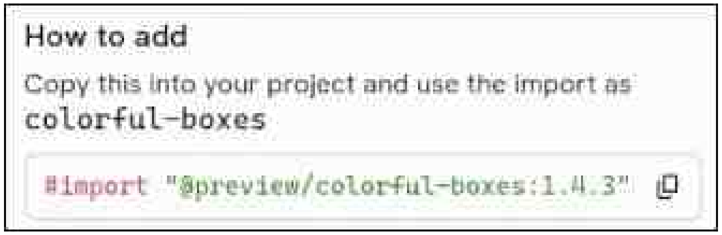


colorful-box

colorful-boxes 1.4.3

Predefined colorful boxes to spice up your document

Next, look for the "How to add" instructions:



How to add

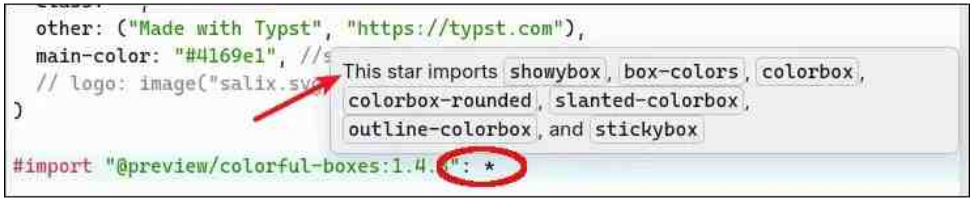
Copy this into your project and use the import as colorful-boxes

```
#import "@preview/colorful-boxes:1.4.3"
```

Click on the "Copy to clipboard" icon to copy the `#import` command for that package. Open your Typst file in the web app—or in your preferred editor, e.g., VSCodium, if you are using Typst locally—and paste the #import command at the beginning of your file. (Now comes the slightly tricky bit.) At the end of the #import command, type " : * " (as shown below):

```
#import "@preview/colorful-boxes:1.4.3": *
```

Importing with " `: *` " at the end of the `#import` statement puts all the content of the `colorful-boxes` package/module into the current scope.



```
  other: ("Made with Typst", "https://typst.com"),
  main-color: "#4169e1", //s
  // logo: image("salix.sv
)

#import "@preview/colorful-boxes:1.4.3": *
```

This star imports `showybox`, `box-colors`, `colorbox`, `colorbox-rounded`, `slanted-colorbox`, `outline-colorbox`, and `stickybox`

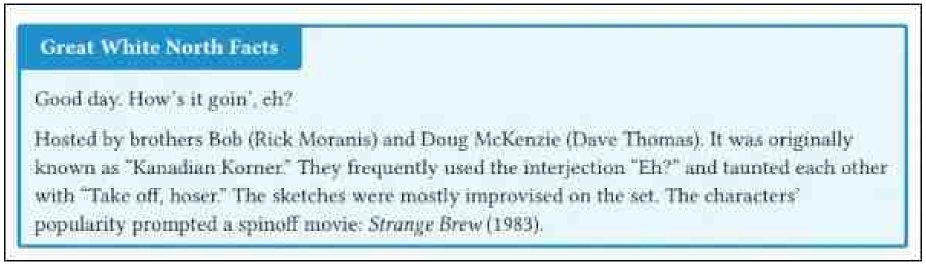
This method is effective for small packages but for large packages with lots of functions, such as `cetz` (for drawing figures and charts), it is better to avoid that and use module import. Otherwise, functions from packages may overlap with yours and each other's. (Thanks to Redditor `Greedy-Vegetable-345` for this technical explanation.) Your package is now available for use. You can read its documentation and/or begin experimenting with examples provided by the package's author.

colorful-boxes

Once you have installed this package (as described above), you can add colorful, customizable boxes to your documents.

These examples illustrate some of the package's capabilities:

```
#colorbox(
title: "Great White North Facts",
color: "blue",
radius: 2pt,
width: auto
)[
Good day. How's it goin', eh?

Hosted by brothers Bob (Rick Moranis) and Doug McKenzie (Dave Thomas). It was originally known as "Kanadian Korner." They frequently used the interjection "Eh?" and taunted each other with "Take off, hoser." The sketches were mostly improvised on the set. The characters' popularity prompted a spinoff movie: _Strange Brew_ (1983).
]
```

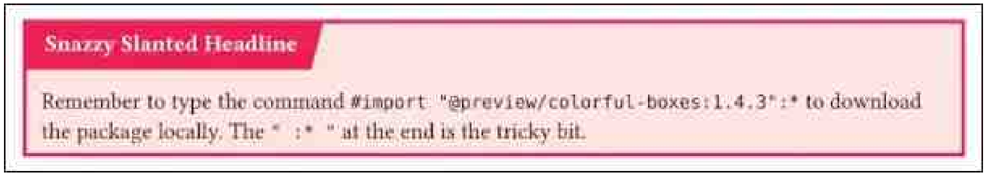


Great White North Facts

Good day. How's it goin', eh?

Hosted by brothers Bob (Rick Moranis) and Doug McKenzie (Dave Thomas). It was originally known as "Kanadian Korner." They frequently used the interjection "Eh?" and taunted each other with "Take off, hoser." The sketches were mostly improvised on the set. The characters' popularity prompted a spinoff movie: *Strange Brew* (1983).

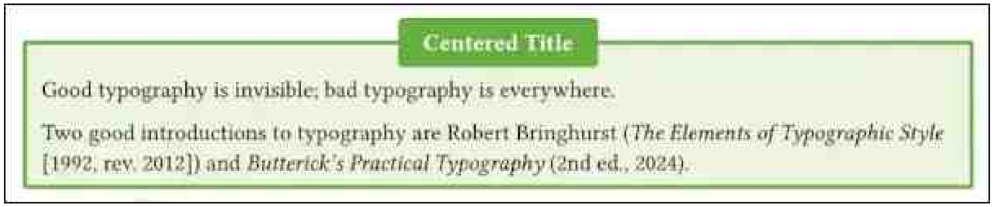
```
#slanted-colorbox(
title: "Snazzy Slanted Headline",
color: "red",
radius: 0pt,
width: auto
)[
Remember to type the command `#import "@preview/colorful-boxes:1.4.3":*` to download the package locally. The `" :* "` at the end is the tricky bit.
]
```



Snazzy Slanted Headline

Remember to type the command #import "@preview/colorful-boxes:1.4.3":* to download the package locally. The " :* " at the end is the tricky bit.

```
#outline-colorbox(
title: "Centered Title",
color: "green",
width: auto,
radius: 2pt,
centering: true
)[
Good typography is invisible; bad typography is everywhere.

Two good introductions to typography are Robert Bringhurst (_The Elements of Typographic Style_ [1992, rev. 2012]) and _Butterick's Practical Typography_ (2nd ed., 2024).
]
```



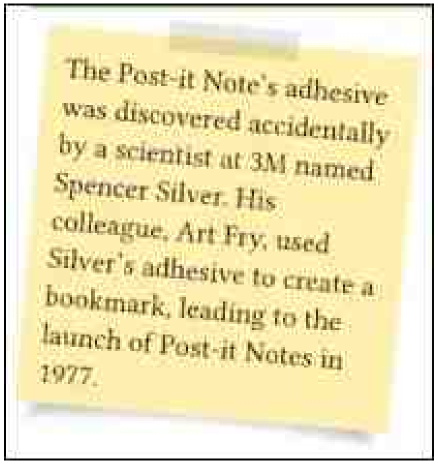
Centered Title

Good typography is invisible; bad typography is everywhere.

Two good introductions to typography are Robert Bringhurst (*The Elements of Typographic Style* [1992, rev. 2012]) and *Butterick's Practical Typography* (2nd ed., 2024).

The "Stickybox" function is fun; it mimics the ubiquitous yellow Post-It Note.

```
#stickybox(
rotation: 5deg,
width: 5cm
)[
The Post-it Note's adhesive was discovered accidentally by a scientist at 3M named Spencer Silver. His colleague, Art Fry, used Silver's adhesive to create a bookmark, leading to the launch of Post-it Notes in 1977.
]
```



The Post-it Note's adhesive was discovered accidentally by a scientist at 3M named Spencer Silver. His colleague, Art Fry, used Silver's adhesive to create a bookmark, leading to the launch of Post-it Notes in 1977.

codly

The codly package is your best choice if you need to embed a lot of code blocks in your document. It allows you to add annotations, skip lines, customize numberings and add programming language icons. Since I am a beginner with codly, I did not change any of the default parameters; I will only cover its most basic usage. For more details, you should consult the author's extensive manual (47 p.) on GitHub.

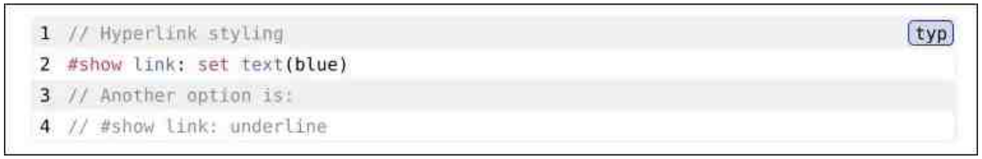
After importing the package, you must initialize it with a #show rule. (You only need to do this once per document.)

```
#import "@preview/codly:1.3.0": *
#import "@preview/codly-languages:0.1.1": *
#show: codly-init.with()
```

By default, `codly` ships with `smart-indent` enabled. This means that `codly` will automatically detect the indentation of your code block and adjust the horizontal offset on line wrapping accordingly.

Adding the Typst code block below will generate the output shown in the screenshot. (The "`typ`" following the three backticks (```` ``` ````) identifies the programming language as Typst.)

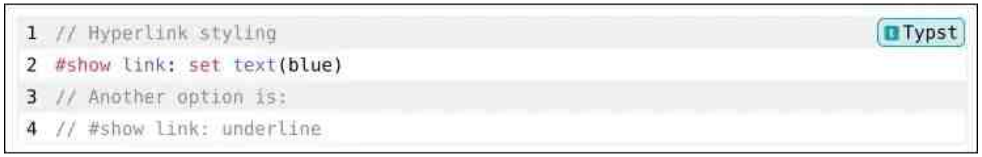
~~~
```typ
// Hyperlink styling
#show link: set text(blue)
// Another option is:
// #show link: underline
```
~~~



```
// Hyperlink styling
#show link: set text(blue)
// Another option is:
// #show link: underline
```

The package ships with language definitions for the Typst language. If you wish, you can use the `typst-icon` function to produce the Typst icon (featuring a miniature Typst logo) for your code blocks:

~~~
#codly(languages: typst-icon)
```typ
// Hyperlink styling
#show link: set text(blue)
// Another option is:
// #show link: underline
```
~~~



```
// Hyperlink styling
#show link: set text(blue)
// Another option is:
// #show link: underline
```

run-liners

The run-liners package allows you to create various sorts of run-in (inline) lists. Its functionality is similar to the paralist package in LaTeX.

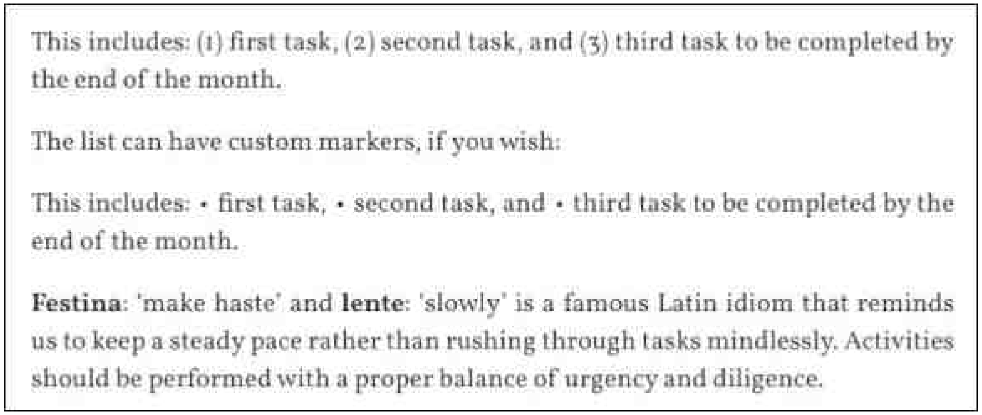
After importing the package, the Typst code below will produce the output shown in the screenshot (next page):

```
This includes: #run-in-enum([first task], [second task], [third task]) to be completed by the end of the month.

The list can have custom markers, if you wish:

This includes:
#run-in-list(
marker: [#sym.circle.filled.small],
[first task],
[second task],
[third task]
)
to be completed by the end of the month.

#run-in-terms(
([Festina], ['make haste']),
([lente], ['slowly'])
)
is a famous Latin idiom that reminds us to keep a steady pace rather than rushing through tasks mindlessly. Activities should be performed with a proper balance of urgency and diligence.
```

There is also an option for run-in lines of poetry, such as this classic haiku by Japanese writer Natsume Sōseki (1867–1916):

```
#run-in-verse(
[The lamp once out],
[Cool stars enter],
```

```
[The window frame.]
)
```

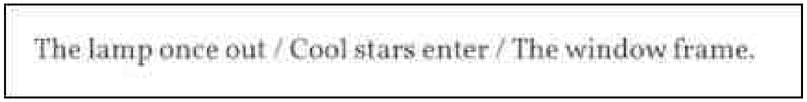


This includes: (1) first task, (2) second task, and (3) third task to be completed by the end of the month.

The list can have custom markers, if you wish:

This includes: • first task, • second task, and • third task to be completed by the end of the month.

Festina: 'make haste' and **lente**: 'slowly' is a famous Latin idiom that reminds us to keep a steady pace rather than rushing through tasks mindlessly. Activities should be performed with a proper balance of urgency and diligence.



The lamp once out / Cool stars enter / The window frame.

untypsignia and metalogo

If you find yourself needing to typeset the logos for TeX and friends, there are two useful packages that work well: `untypsignia` and `metalogo`. Their usage is straightforward; you will be able to understand them from the examples provided by their authors.

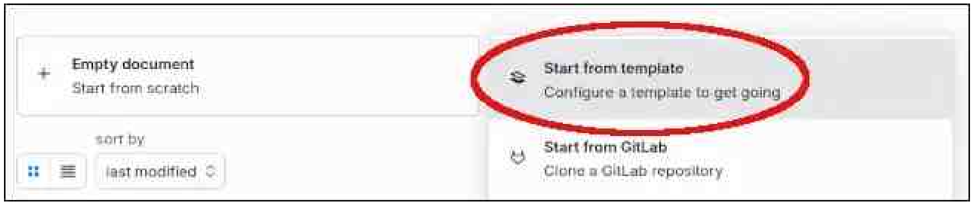
basic-report Template

For a report format with a clean, professional look, I recommend the `basic-report` template by Roland Schätzle. It was designed to include an attractive title page, a table of contents page and content pages (supporting three levels of headings). The template uses the Vollkorn (serif) font for the body text; the Ubuntu font (sans serif) is used as a contrasting companion font for the title page, table of contents, headings, and labels.

I created a brief document (7 p.) with the basic-report template and have shared it as a project (read-only access) from Typst's web app, to provide a glimpse of the results that you can expect. The user guide for Acme™ rocket-powered roller skates is tongue in cheek—unless you are a hungry coyote in pursuit of a roadrunner.

In case you have not used a template from Typst Universe before, here are quick instructions:

- In the Typst web app, click on the "Start from template" option in the Dashboard, then search for basic-report.



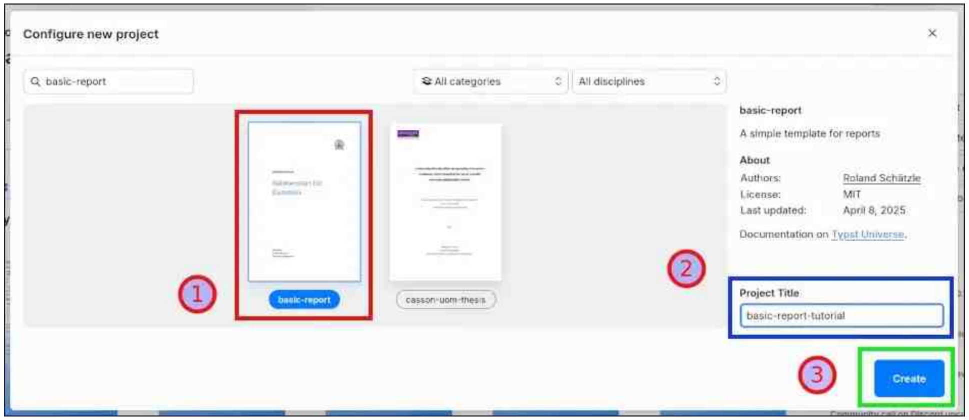
Empty document
Start from scratch

Start from template
Configure a template to get going

Start from GitLab
Clone a GitLab repository

sort by
last modified

- When the search results are displayed, click on the basic-report page icon to select it. Give your project a title, then click on the Create button.



Configure new project

basic-report

All categories

All disciplines

basic-report

A simple template for reports

About

Authors: Roland Schätzle
License: MIT
Last updated: April 8, 2025

Documentation on Typst Universe.

Project Title
basic-report-tutorial

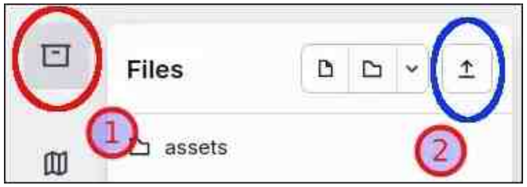
One quirk with using this template is that although Vollkorn comes pre-installed in the Typst web app, the Ubuntu font does not. Therefore, you must import the font into your project. That can be accomplished easily following the steps below:

- Download the Ubuntu font via Google Fonts or from the 1001 Fonts website. The Ubuntu font family is distributed at no cost, under an open/libre license.

- If you download via Google Fonts, you will have a `.zip` file which you will need to extract. The unzipped folder will include several fonts; the most versatile choice is the `Ubuntu-Regular.ttf` file.

- If you download from 1001 Fonts, you can select just the "Ubuntu Regular" variant (which will download a file named `ubuntu.regular.ttf`).

- In Typst's web app, click on the `Explore files` icon, then click on the `Upload a new file` button to upload your desired `.ttf` file.

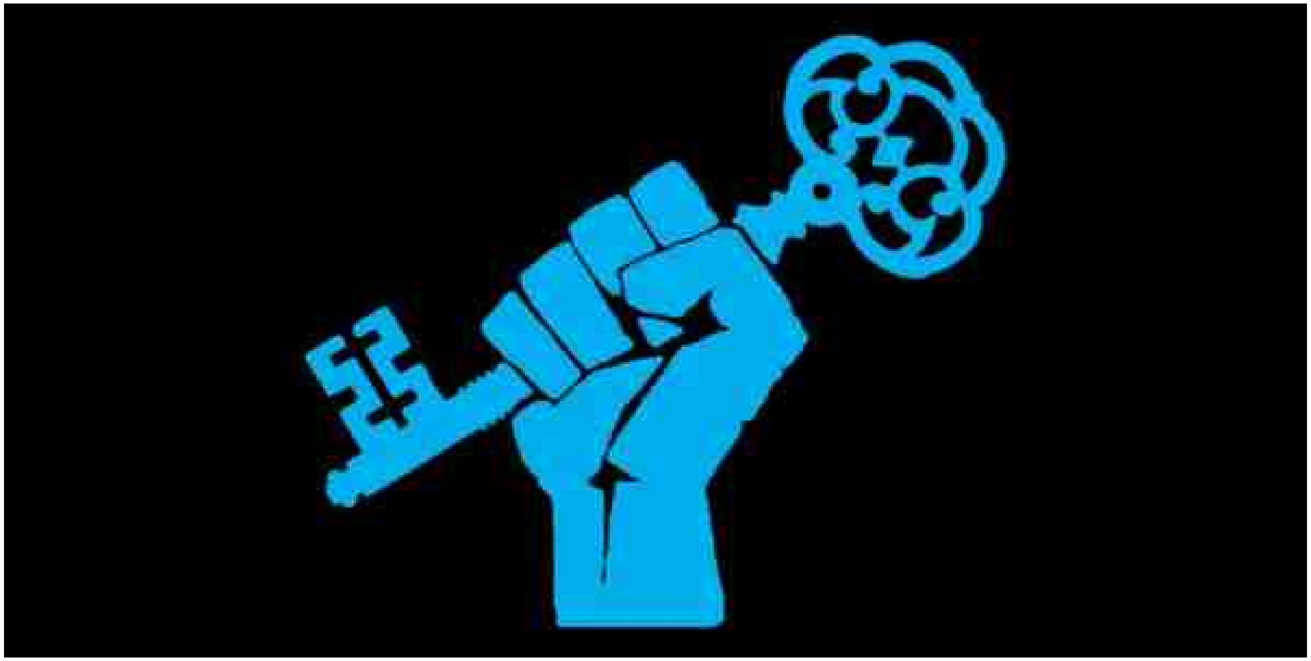


- The new font will be discovered automatically. You should see the font on the title page, table of contents and the headings change from Vollkorn to Ubuntu Regular.

If you are using the Typst compiler locally on your PCLinuxOS system, the procedure for setting up the `basic-report` template is slightly different. I have written separate instructions for that in my shared project, in case you are interested.

I hope these tips will boost your productivity with Typst and encourage you to continue exploring its capabilities. I am working on the third (and final) part of this cookbook series, which will focus on creating title pages with Typst. If you are interested in seeing a Typst-generated replica of this article, I have publicly shared my project. The document's body typeface is Source Serif Pro, and the headings use Source Sans Pro.

A Win for Encryption: France Rejects Backdoor Mandate



by Joe Mullin
Electronic Frontier Foundation

In a moment of clarity after initially moving forward a deeply flawed piece of legislation, the French National Assembly has done the right thing: it rejected a dangerous proposal that would have gutted end-to-end encryption in the name of fighting drug trafficking. Despite heavy pressure from the Interior Ministry, lawmakers voted (article in French) to strike down a provision that would have forced messaging platforms like Signal and WhatsApp to allow hidden access to private conversations.

The vote is a victory for digital rights, for privacy and security, and for common sense.

The proposed law was a surveillance wishlist disguised as anti-drug legislation. Tucked into its text was a resurrection of the widely discredited “ghost” participant model — a backdoor that pretends not to be one. Under this scheme, law enforcement could silently join encrypted chats, undermining the very idea of private communication. Security experts have condemned the approach, warning it would introduce systemic vulnerabilities, damage trust in secure communication platforms, and create tools ripe for abuse.

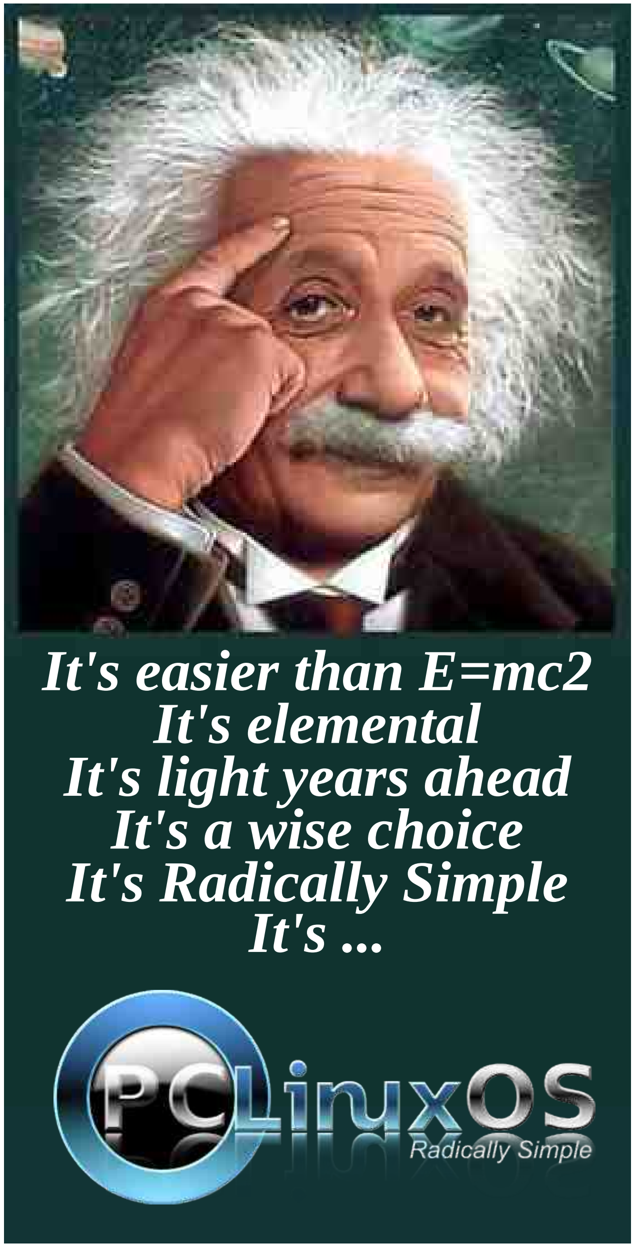
The French lawmakers who voted this provision down deserve credit. They listened — not only to French digital rights organizations and technologists, but also to basic principles of cybersecurity and civil liberties. They understood that encryption protects everyone, not just activists and dissidents, but also journalists, medical professionals, abuse survivors, and ordinary citizens trying to live private lives in an increasingly surveilled world.

A Global Signal

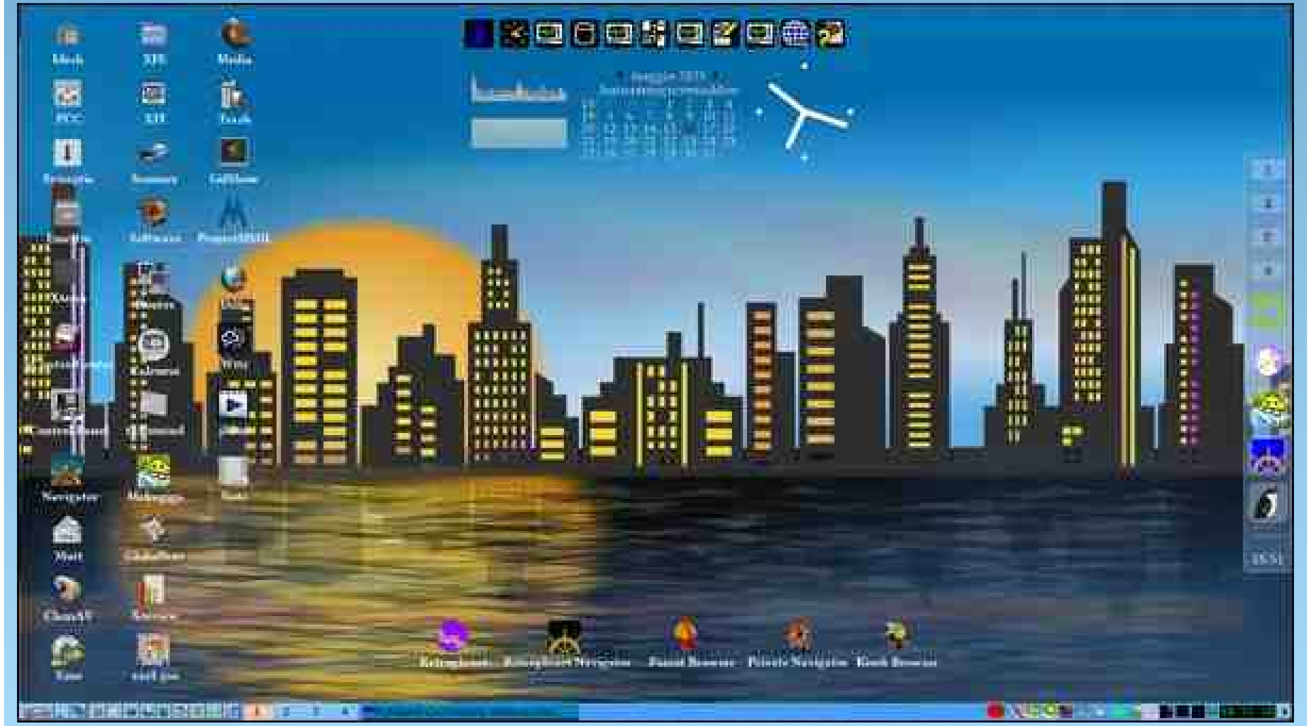
France’s rejection of the backdoor provision should send a message to legislatures around the world: you don’t have to sacrifice fundamental rights in the name of public safety. Encryption is not the enemy of justice; it’s a tool that supports our fundamental human rights, including the right to have a private conversation. It is a pillar of modern democracy and cybersecurity.

As governments in the U.S., U.K., Australia, and elsewhere continue to flirt with anti-encryption laws, this decision should serve as a model — and a warning. Undermining encryption doesn’t make society safer. It makes everyone more vulnerable.

This victory was not inevitable. It came after sustained public pressure, expert input, and tireless advocacy from civil society. It shows that pushing back works. But for the foreseeable future, misguided lobbyists for police national security agencies will continue to push similar proposals—perhaps repackaged, or rushed through quieter legislative moments.



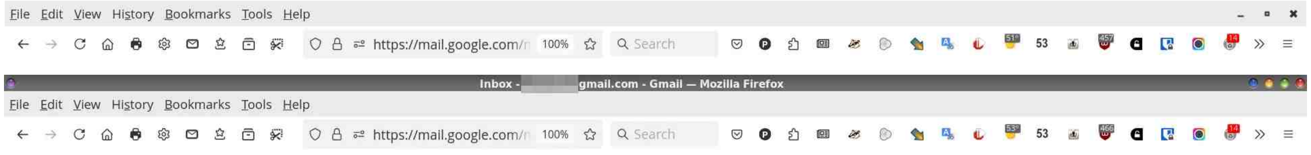
Screenshot Showcase



Posted by francesco bat, May 16, 2025, running IceWM.

Restore Firefox Title Bar

by Paul Arnote (parnote)


File Edit View History Bookmarks Tools Help
https://mail.google.com/
100%
Search
Inbox - [redacted]gmail.com - Gmail — Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://mail.google.com/
100%
Search

Top: Firefox without title bar   Bottom: Firefox with title bar

I don't even try to keep it a secret. I'm a HUGE Firefox fan. The fact that my only other choice these days is a Chromium-based browser (such as Chrome, Chromium, Brave, Opera, Edge, and a whole host of other browsers), doesn't even give me much of a real choice at all. I've also not even attempted to hide my disdain for those "other" browsers. See, I've been a Firefox user since its inception. And don't even get me started on how much of a HOG the Chromium-based browsers are, both in CPU cycles and memory usage. Plus, I can't "push" the Chromium-based browsers the way that I "push" Firefox. If I were to have as many open tabs in a Chromium-based browser like I tend to sometimes have in Firefox, the Chromium-based browsers will bring my entire system to a literal crawl, sometimes even locking up my system.

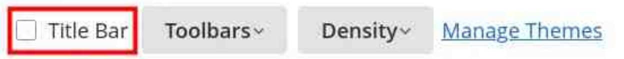
Yes, I have Chromium-based browsers installed (specifically, Chromium-Ungoogled, Chrome, Opera, and Brave) for accessing those poorly designed sites that ONLY display properly on a Chromium-based browser. In many ways, it reminds me of the "Internet Explorer" days, when Microsoft tried to commandeer the browser market with that albatross. In case you don't remember, Microsoft tried to use their position in the operating system market to dictate what the W3 standards "should be." There were sites that were written to be "best viewed" by Internet Explorer, the W3 to be damned. Fortunately for us all, that push by Microsoft failed as miserably as Internet Explorer was buggy.

So, you can imagine my horror/surprise when I recently ran updates from Synaptic. One of those programs being updated was Firefox. When I relaunched Firefox, it was missing the title bar decoration at the top of the Firefox window!

My initial thoughts were that Firefox crawled down that same tainted rabbit hole that the Chromium-based browsers did. Perish the thought!

I've become accustomed over the years to relying on the information displayed in the title bar to help keep me oriented as to which page I'm currently looking at. This is an especially expedient way for me to keep my bearings as to what page I'm currently viewing, especially when I have a LOT of tabs opened up at the same time (as I often have when I'm working on magazine articles).

I first visited Firefox's **about:config** settings page, but I wasn't able to quickly or easily discern which setting regulated the display of the title bar. A subsequent and quick internet search led me to an almost 11-year-old post on Mozilla's support website. Fortunately, it's a super easy fix.



Go to Firefox's "Hamburger" menu, and select "More Tools" (found near the bottom of the hamburger menu). From there, select "Customize Toolbar." In the far bottom left of that window, place a checkmark in the checkbox that's labeled "Title Bar" (outlined in red in the image above).

Voilà! My precious title bar has returned! And, no restart is required.

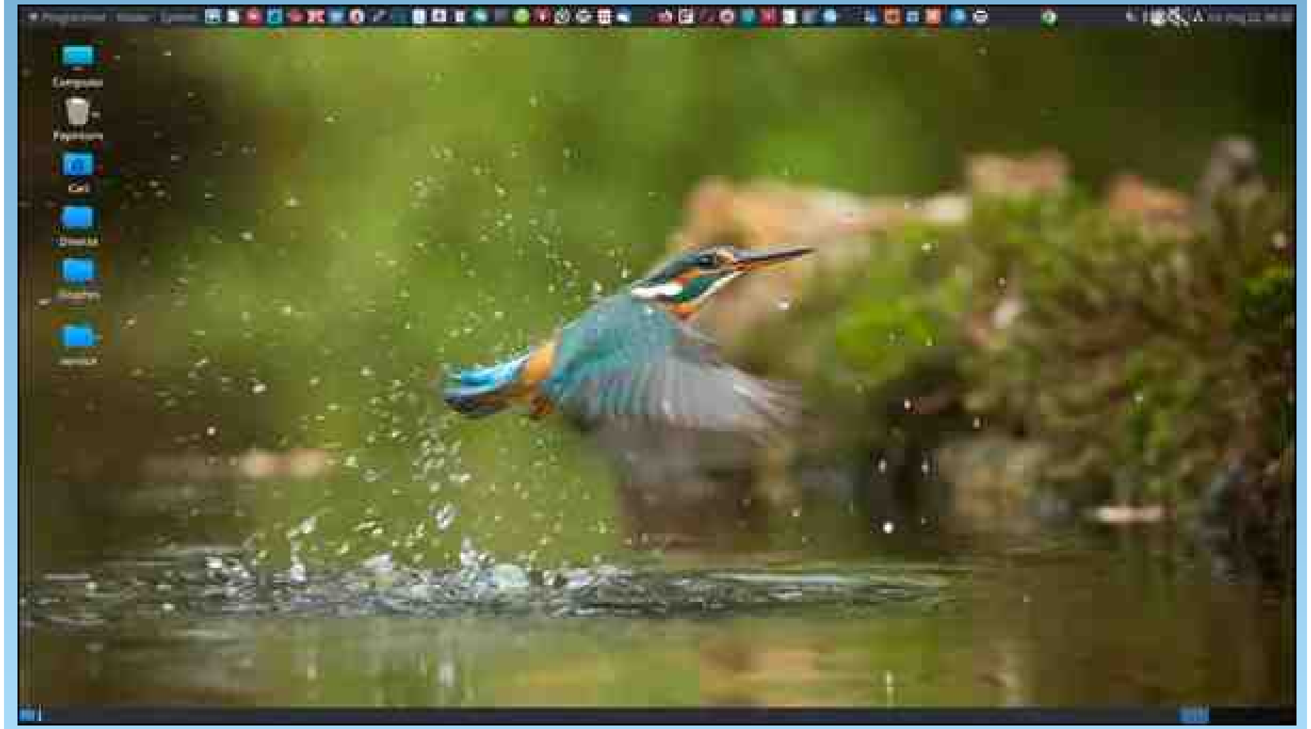
It seems that when I updated to Firefox 138.0, that setting wasn't carried over/transferred to the updated version of Firefox, for some unknown reason.

Phew! Crisis averted!

As a side note, I also have the Midori browser installed, which uses the Mozilla web engine. In fact, Midori tends to use the Firefox settings. So, for a brief time, Midori exhibited the same behavior as Firefox, appearing without a title bar. So, the same setting is also available in Midori, in exactly the same location. While I don't have these installed and don't use these programs, I understand that Mercury browser and Thunderbird also have this same setting. If you use either of those, the "fix" should apply to those, as well.

So, if you're a Firefox user (or a Midori user) and found yourself in the same predicament, rest assured that you can "put things right" again very easily and very quickly. This is just one of the many reasons I love Firefox!

Screenshot Showcase



Posted by Snubbi, May 22, 2025, running Mate.

Good Words, Good Deeds, Good News

compiled by Meemaw

Ten-Year-old Boy Gifts Easter Baskets To Needy

Ten-year-old Carl and his mother have been giving out Easter baskets to the needy in Memphis, TN for the last six years. They started in 2020 when many were out of work due to COVID. Carl says the tradition means a lot to him. *“Sometimes I just want to cry,” he explained, “because I’ve helped so many people who are in need and less fortunate.”*

This year it was an event which included the Easter Bunny. Carl and his mother handed out 300 baskets. Many other cities have individuals who do the same thing. A church in San Antonio, TX and a motorcycle dealership in St. Charles LA gave away Easter baskets this year as well.

Man Finds 3.81 Carat Diamond

David regularly visits the Crater of Diamonds State Park in Arkansas, traveling from his home in Minnesota. He visited the park in April, and while he was there, he saw something shiny on the ground that appeared to be a candy wrapper. However, the closer he got to it, the less it looked like a wrapper. Before he even picked it up, he knew it was a diamond.

When he showed it to the park personnel, they registered it as a 3.81 carat diamond. He was really surprised to find one that large. “*You just never know what you’re gonna find. It’s a chance of a lifetime,” he said*, adding it would probably never happen again for him but maybe for the next person.

From the park’s website, *The only place in the world where the public can search for real diamonds in their original volcanic source, Crater of Diamonds is a one-of-a-kind experience that brings people from all over the world to Murfreesboro, Arkansas. Visitors to the park search a 37-acre field, the eroded surface of a volcanic crater, for a variety of rocks, minerals, and gemstones – and any rock or mineral you find is yours to keep.*

Arizona Ranch Dog Guides Toddler To Safety

Two year-old Boden wandered away from his home in Seligman, AZ, one afternoon in April, and the community and police organized a 16-hour search. However, he was found seven miles away near Kingman, AZ. Scotty’s dog, Buford, found the child on Scotty’s ranch and was escorting him up to the house.

This is an area where wildlife sightings are frequent. Bears, coyotes, snakes and mountain lions are plentiful in the area. In fact, when officers did a thermal scan of the area during the search, the scanners found two mountain lions.

According to Scotty, the child followed a power line to his property. The boy told him he slept under a tree and the dog found him. The rancher also explained that Buford is an Anatolian Pyrenees whose purpose is to safeguard his family. *"He goes out at night and just kind of patrols. He goes half a mile, a mile from the house and just makes big loops, keeps coyotes out," he noted.*

Police Officer Saves Child Despite His Fear Of Heights

A Philadelphia, PA, police officer put aside his fears when a 911 call came in about a child on the roof of a house. Officer Eric rushed to the neighborhood to try to help. He had always been afraid of heights, but had to do something. He rushed into the house, notifying an adult in the house that the child was on the roof. The parents weren't aware because a neighbor had called it in. He climbed out onto the roof and took the child back into the house.

"I just locked onto the kid and started trying to map out how I can safely grab the kid without startling him and him possibly falling over the edge of the roof. I don't even think he knew I was there," the officer explained. *"Instantly overcoming my fear of heights and getting him off the roof… it hit home because it could have been my kid and I would want someone to do the same."*

Mail Carrier Saves Child From Dog Mauling

Letter carrier Rungphet was delivering mail and noticed that a school bus had stopped nearby. She suddenly heard screams and saw that a dog had attacked a girl after she got off the bus. The dog had bitten on the girl's leg and was trying to drag her away. A woman in the neighborhood was trying to get the girl away from the dog. Rungphet stopped her truck, grabbed her dog spray and went to help. She had to spray the dog several times before it backed off, then she pulled her truck between the child and the dog while the neighbor helped the child.

The ambulance was called, and the child was taken to the hospital, where she underwent several surgeries. She had suffered many bites, almost losing her arm. However, she was back at school about a month later. The dog had to be euthanized.

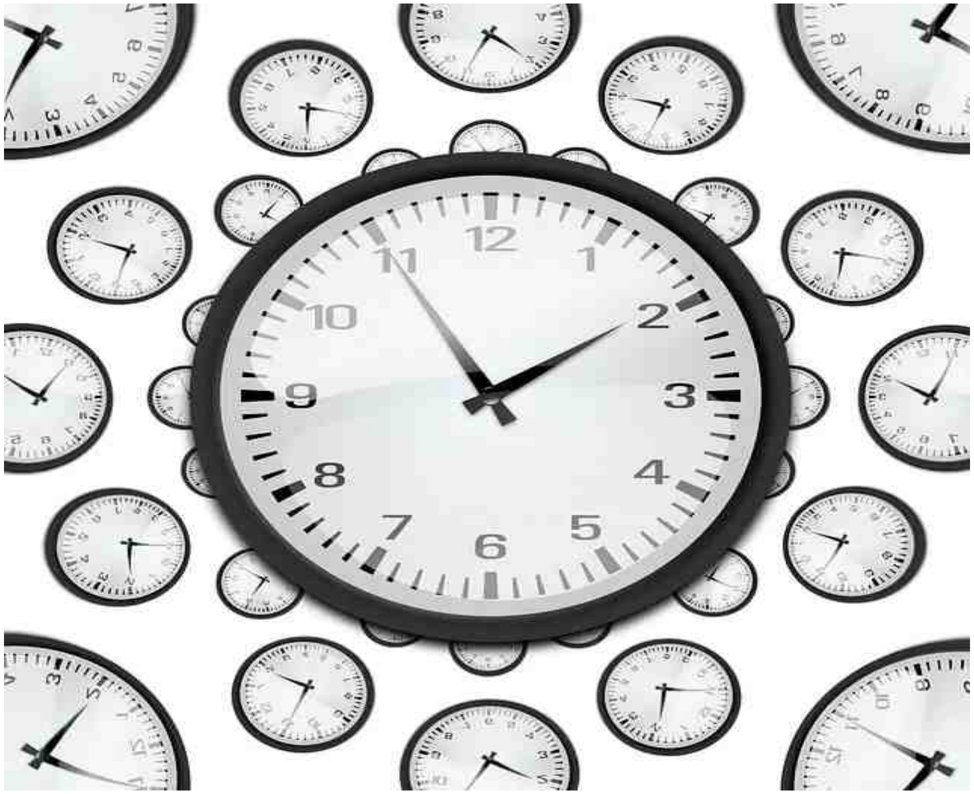
Rungphet received an award for her actions. *Following the harrowing incident, she said of the child, "She comes up to me and gives me hugs. Every time she sees the mail truck, she comes running. That's the best."*

Wiki Pick: The Wrong Time Is Displayed In Windows On A Dual Boot Computer With Linux

by Dave Marshall (CoreLite)

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

This works for any version of PCLinuxOS (and most other non-systemd Linux distros) when dual booting Windows 10 or 11.



After installing Linux to dual boot with Windows, the wrong time appears on the Taskbar when you boot back into Windows. Linux and Windows both get the time from the same source. The computer has two primary clocks – the hardware clock and the system clock. The system clock is what you see on the taskbar. The hardware clock is the motherboard clock that you set up in the UEFI/BIOS. When you boot the computer up, the system clock reads the time from the hardware clock and keeps time until the computer is shut down. When the computer shuts down, the system clock writes the time to the hardware clock.

The problem is caused by the different way that the two operating systems calculate the time based on that reading from the hardware clock. Windows sees the time from the hardware clock as Local Time, which is the time that you set in the BIOS. Linux sees the hardware clock time as UTC (Universal Time), and then calculates the local time from the Time Zone that you selected during the installation. In my case, the local time is UTC minus 5 hours. If my hardware clock shows 12:00 noon, Linux thinks that is UTC and calculates local time. At shut down, Linux syncs the hardware clock to UTC, or 5:00 PM. When you shutdown Linux and boot into Windows, Windows sees the hardware clock showing 5:00 PM and thinks that is local time, when in fact, it is 5 hours ahead.

There are a few different ways to fix this problem. Fixing it in Windows requires a Registry hack. We won't go there. One way to fix it in Linux involves changing /etc/adjtime with a text editor. The easy way to fix it is a simple one line command in Konsole.

Log in to Linux as root and enter this command: **hwclock -w -l**

That has the same effect as editing /etc/adjtime.

You will not see a change on your Linux desktop, but the next time you boot into Windows, you will see the correct time on the taskbar.

You can view the original PCLinuxOS Knowledgebase Wiki article here. Image by Gerd Altmann from Pixabay.

U.S. Appeals Court Sidesteps The Big Questions On Geofence Warrants

by Andrew Crocker
Electronic Frontier Foundation

Another federal appeals court has ruled on controversial geofence warrants — sort of. Last week, the US Court of Appeals for the Fourth Circuit sitting en banc issued a single sentence opinion affirming the lower court opinion in United States v. Chatrie. The practical outcome of this sentence is clear: the evidence collected from a geofence warrant issued to Google can be used against the defendant in this case. But that is largely where the clarity ends, because the fifteen judges of the Fourth Circuit who heard the en banc appeal agreed on little else. The judges wrote a total of nine separate opinions, no single one of which received a majority of votes. Amid this fracture, the judges essentially deadlocked on important constitutional questions about whether geofence warrants are a Fourth Amendment search. As a result, the new opinion in Chatrie is a missed opportunity for the Fourth Circuit to join both other appellate courts to have considered the issue in finding geofence warrants unconstitutional.

Geofence warrants require a provider — almost always Google — to search its entire reserve of user location data to identify all users or devices located within a geographic area and time period, both specified by law enforcement. This creates a high risk of suspicion falling on innocent people and can reveal sensitive and private information about where individuals have traveled in the past. Following intense scrutiny from the press and the public, Google announced changes to how it stores location data in late 2023, apparently with the effect of eventually making it impossible for the company to respond to geofence warrants.

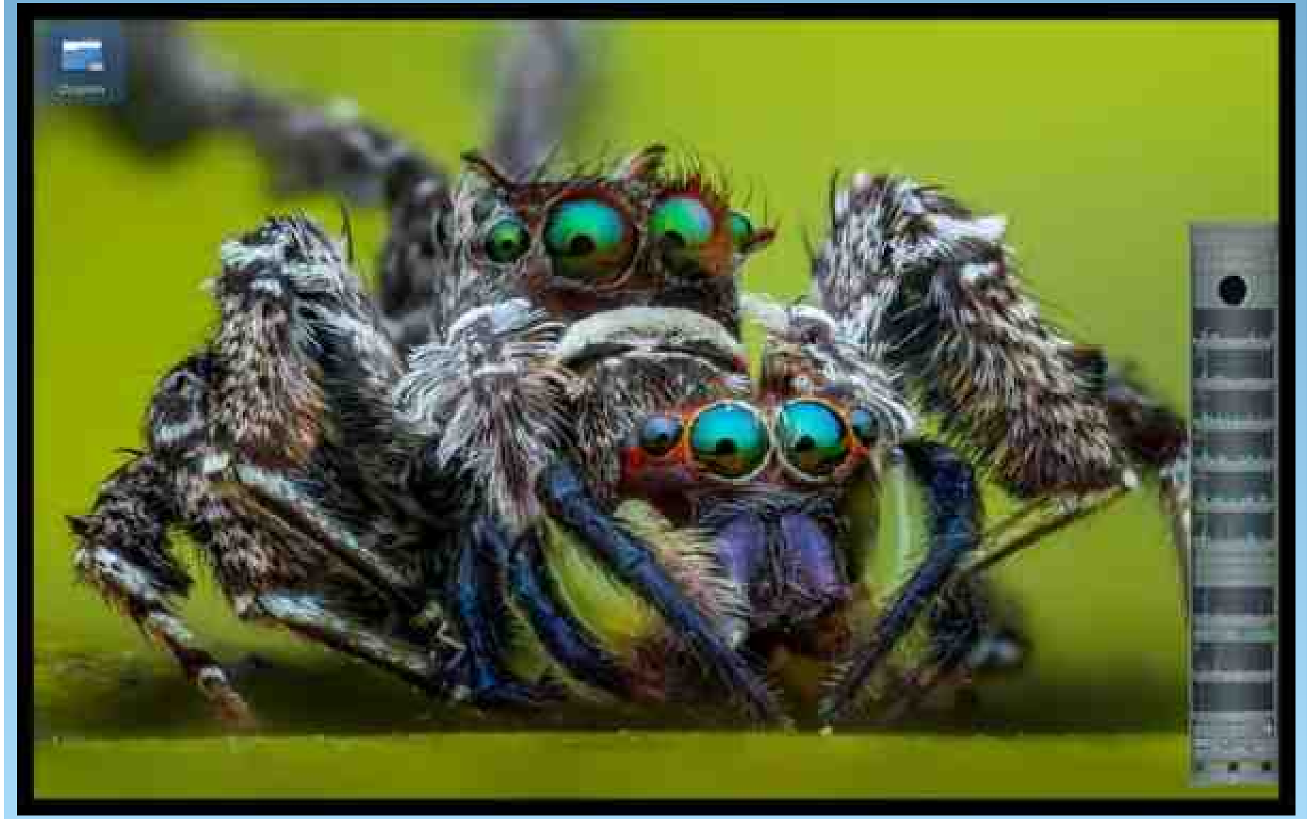
Regardless, numerous criminal cases involving geofence evidence continue to make their way through the courts. The district court decision in Chatrie was one of the first, and it set an important precedent in finding the warrant overbroad and unconstitutional. However, the court allowed the government to use the evidence it obtained because it relied on the warrant in “good faith.” On appeal, a three judge panel of the Fourth Circuit voted 2-1 that the geofence warrant did not constitute a search at all. Later, the appeals court agreed to rehear the case en banc, in front of all active judges in the circuit. (EFF filed amicus briefs at both the panel and en banc stages of the appeal).

The only agreement among the fifteen judges who reheard the case was that the evidence should be allowed in, with at least eight relying on the good faith analysis. Meanwhile, seven judges argued that geofence warrants constitute a Fourth Amendment search in at least some fashion, while exactly seven disagreed. Although that means the appellate court did not rule on the Fourth Amendment implications of geofence warrants, neither did it vacate the lower court’s solid constitutional analysis.

Above all, it remains the case that every appellate court to rule on geofence warrants to date has found serious constitutional defects. As we explain in every brief we file in these cases, reverse warrants like these are very sort of “general searches” that the authors of the Fourth Amendment sought to prohibit. We’re dedicated to fighting them in courts and legislatures around the country.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

Screenshot Showcase



Posted by The CrankyZombie, May 1, 2025, running KDE.

Site-Blocking Legislation Is Back. It's Still A Terrible Idea.

by Joe Mullin
Electronic Frontier Foundation

More than a decade ago, Congress tried to pass SOPA and PIPA — two sweeping bills that would have allowed the government and copyright holders to quickly shut down entire websites based on allegations of piracy. The backlash was immediate and massive. Internet users, free speech advocates, and tech companies flooded lawmakers with protests, culminating in an "Internet Blackout" on January 18, 2012. Turns out, Americans don't like government-run internet blacklists. The bills were ultimately shelved.

Thirteen years later, as institutional memory fades and appetite for opposition wanes, members of Congress in both parties are ready to try this again.

The Foreign Anti-Digital Piracy Act (FADPA), along with at least one other bill still in draft form, would revive this reckless strategy. These new proposals would let rights holders get federal court orders forcing ISPs and DNS providers to block entire websites based on accusations of infringing copyright. Lawmakers claim they're targeting "pirate" sites—but what they're really doing is building an internet kill switch.

These bills are an unequivocal and serious threat to a free and open internet. EFF and our supporters are going to fight back against them.

Site-Blocking Doesn't Work—And Never Will

Today, many websites are hosted on cloud infrastructure or use shared IP addresses. Blocking one target can mean blocking thousands of unrelated sites. That kind of digital collateral damage has already happened in Austria, Russia, and in the US.

Site-blocking is both dangerously blunt and trivially easy to evade. Determined evaders can create the same content on a new domain within hours. Users who want to see blocked content can fire up a VPN or change a single DNS setting to get back online.

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

These workarounds aren't just popular—they're essential tools in countries that suppress dissent. It's shocking that Congress is on the verge of forcing Americans to rely on the same workarounds that internet users in authoritarian regimes must rely on just to reach mislabeled content. It will force Americans to rely on riskier, less trustworthy online services.

Site-Blocking Silences Speech Without a Defense

The First Amendment should not take a back seat because giant media companies want the ability to shut down websites faster. But these bills wrongly treat broad takedowns as a routine legal process. Most cases would be decided in ex parte proceedings, with no one there to defend the site being blocked. This is more than a shortcut – it skips due process entirely.

Users affected by a block often have no idea what happened. A blocked site may just look broken, like a glitch or an outage. Law-abiding publishers and users lose access, and diagnosing the problem is difficult. Site-blocking techniques are the bluntest of instruments, and they almost always punish innocent bystanders.

The copyright industries pushing these bills know that site-blocking is not a narrowly tailored fix for a piracy epidemic. The entertainment industry is booming right now, blowing past its pre-COVID projections. Site-blocking legislation is an attempt to build a new American censorship system by letting private actors get dangerous infrastructure-level control over internet access.

EFF and the Public Will Push Back

FADPA is already on the table. More bills are coming. The question is whether lawmakers remember what happened the last time they tried to mess with the foundations of the open web.

If they don’t, they’re going to find out the hard way. Again.

Site-blocking laws are dangerous, unnecessary, and ineffective. Lawmakers need to hear — loud and clear — that Americans don’t support government-mandated internet censorship. Not for copyright enforcement. Not for anything.

Reach Us On The Web

PCLinuxOS Magazine Mailing List
https://groups.google.com/group/pclinuxos-magazine
PCLinuxOS Magazine Web Site
https://pclosmag.com/
PCLinuxOS Magazine Forums
https://www.pclinuxos.com/forum/index.php?board=34.0

Screenshot Showcase

Posted by bliss, May 18, 2025, running KDE.

PCLinuxOS Recipe Corner Bonus

Grilled Chicken Bites with Creamy Garlic Sauce

Serves: 4

INGREDIENTS:

For the Chicken:
1 lb boneless, skinless chicken breasts,
cut into 1-inch cubes
1 tablespoon olive oil
1 teaspoon paprika
1/2 teaspoon garlic powder
1/4 teaspoon salt
1/4 teaspoon black pepper
1/4 teaspoon cayenne pepper (optional)

For the Creamy Garlic Sauce:
1/2 cup mayonnaise
1/4 cup sour cream
2 cloves garlic, minced
1 tablespoon chopped parsley
1 teaspoon lemon juice
1/4 teaspoon salt
1/4 teaspoon black pepper

DIRECTIONS:

Prep the Chicken: In a bowl, combine chicken cubes, olive oil, paprika, garlic powder, salt, pepper, and cayenne pepper (if using). Toss to coat.

Grill the Chicken: Grill the chicken cubes over medium heat for 2-3 minutes per side, or until cooked through.

Make the Creamy Garlic Sauce: In a small bowl, whisk together mayonnaise, sour cream, garlic, parsley, lemon juice, salt, and pepper.

Serve: Arrange grilled chicken bites on a platter and drizzle with Creamy Garlic Sauce.

TIPS & TWEAKS:

Spice it up: Add more cayenne pepper or a pinch of red pepper flakes to the chicken marinade.

Make it a meal: Serve chicken bites with a side of rice, pasta, or vegetables.

Garnish with fresh parsley or chives.

NUTRITION:

Calories: 320	Carbs: 2g	Sodium: 490mg
Fiber: 0g	Protein: 26g	

PCLinuxOS Puzzled Partitions

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

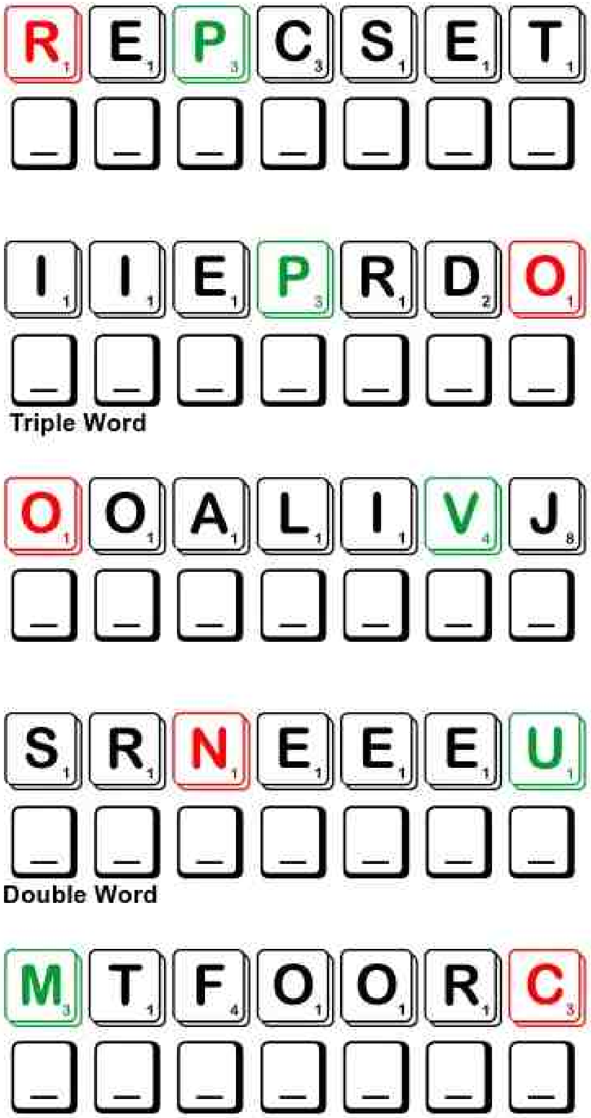
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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 222, average score 155.

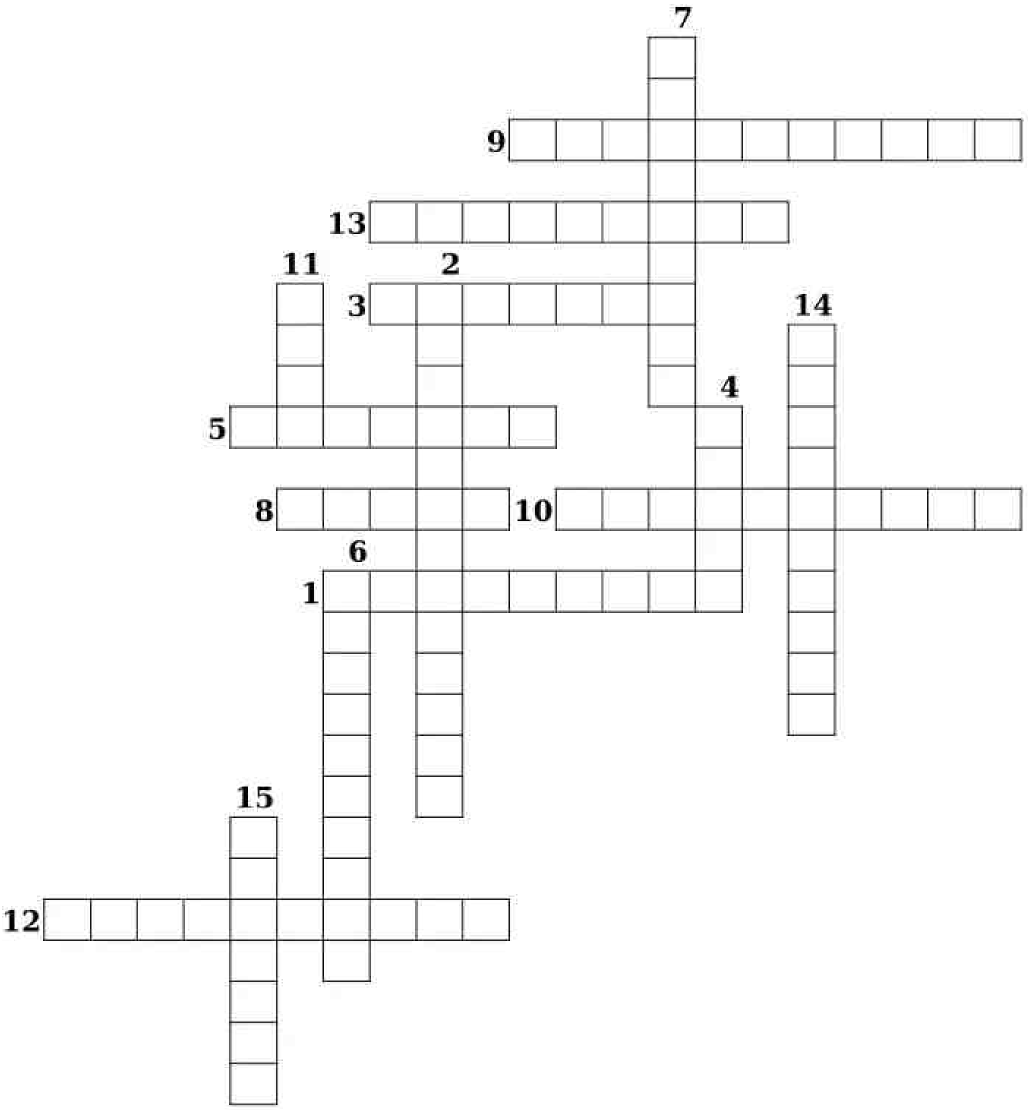
June 2025 Word Find
Father's Day Feelings

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

Admiration	Affection
Appreciation	Belonging
Blessed	Bonding
Care	Cheerful
Comfort	Connection
Contentment	Empathy
Encouragement	Endearment
Enthusiasm	Fondness
Generosity	Gladness
Gratitude	Happiness
Inspiration	Kindhearted
Kindness	Love
Nostalgia	Nurture
Optimism	Pride
Reassurance	Respect
Support	Sympathy
Trust	Understanding

Download Puzzle Solutions Here

June 2025 Crossword
Father's Day Feelings



1. The feeling or quality of being thankful and appreciative for the kindness or help received from others.
2. The mental grasp or comprehension of a subject, situation, or concept.
3. The process of caring for and encouraging the growth or development of someone or something.
4. A feeling of pleasure and satisfaction derived from ones achievements.
5. A positive feeling or action shown towards someone or something that is considered important or held in high esteem.
6. The quality of being willing to give help or support, often more than is usual or expected, without expecting anything in return.
7. A state of well-being and contentment, often characterized by feelings of joy and satisfaction.
8. The belief that someone or something is reliable, good, honest, and effective.
9. The process of being mentally stimulated to do or feel something creative or important.
10. A feeling of respect and approval towards someone or something, often accompanied by a sense of wonder or delight.
11. A strong feeling of affection and emotional attachment towards someone or something.
12. A linking or joining two or more things, or a relationship or association between people, ideas, or events.
13. A feeling of liking and caring for someone or something.
14. A word or act that expresses affection.
15. Honored in worship or enjoying happiness, often associated with divine favor or good fortune.

Download Puzzle Solutions Here

Mixed-Up-Meme Scrambler

NOMUT _ _ □ _ □

LAROF _ _ □ □ _

CELLOA □ _ □ _ □ _

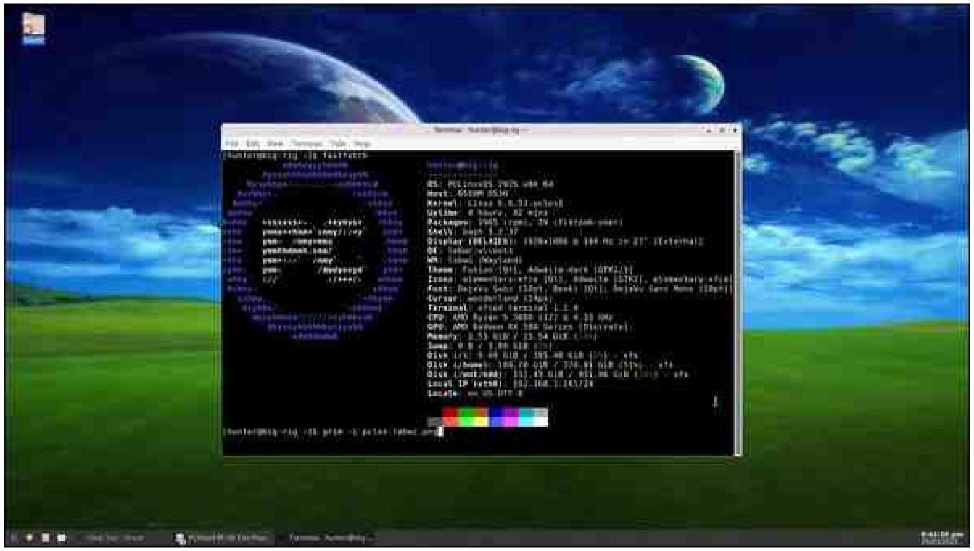
CIANAM _ □ _ _ □ □

Counts when shopping for a car...

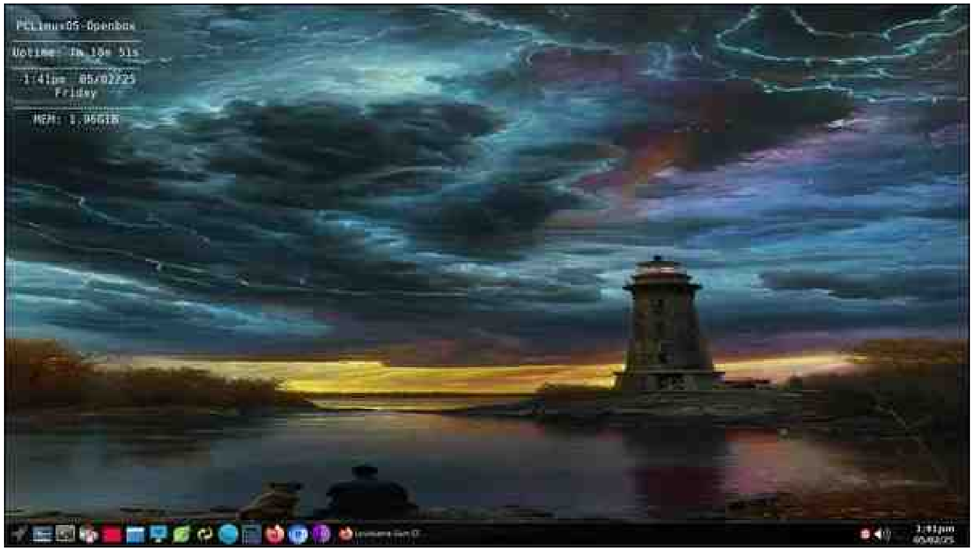
A _ _ _ _ _ _ _ _ _ _

Download Puzzle Solutions Here

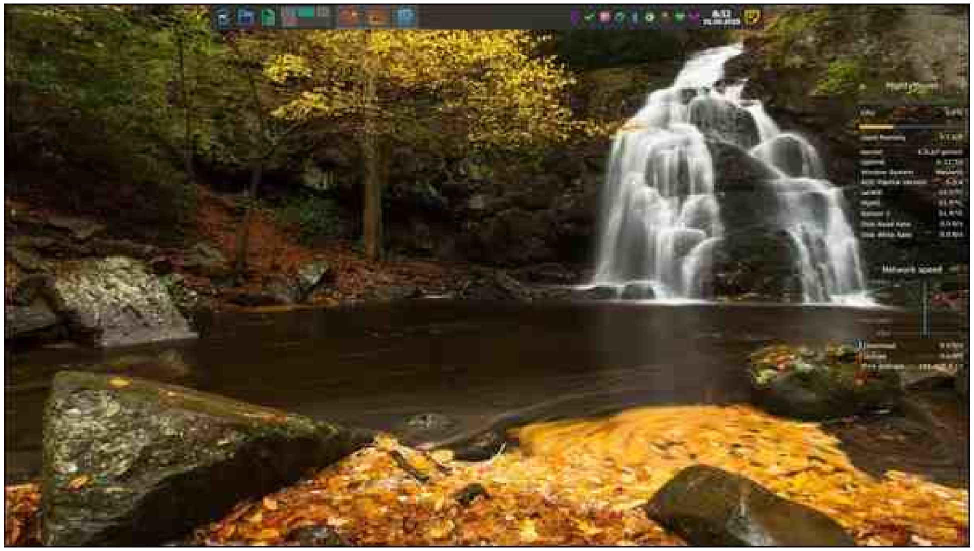
More Screenshot Showcase



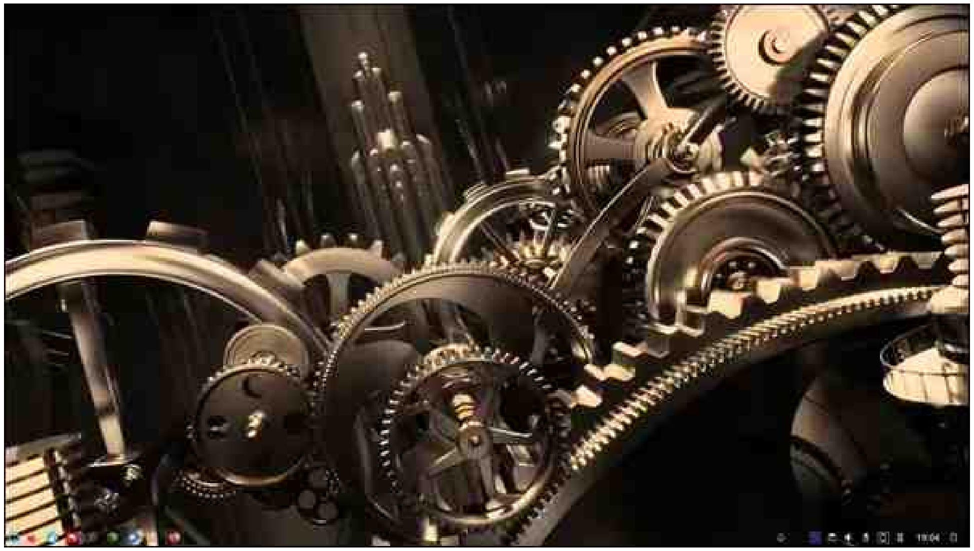
Posted by hunter0ne, May 1, 2025, running KDE.



Posted by astronaut, May 2, 2025, running Openbox.



Posted by tbs, May 1, 2025, running KDE.



Posted by luikki, May 2, 2025, running KDE.