

The PCLinuxOS magazine

Volume 214

November, 2024



ICYMI: How To Tell If Someone Is Telling You The Truth

*GIMP Tutorial:
Create A Double Exposure*

*PCLinuxOS Wiki
Knowledgebase Resurrected!*

*Tip Top Tips: Backing Up Your
/home Directory*

*PCLinuxOS Recipe Corner:
Skillet Coq Au Vin for Two*

New NIST Password Guidelines

*Exploring Typst:
A LaTeX Alternative*

*How To Stop Advertisers From
Tracking Your Teen Across The
Internet*

And more inside...

Inside This Issue...

- 3 From The Chief Editor's Desk**
- 4 Screenshot Showcase**
- 5 ICYMI: How To Tell If Someone Is Telling You The Truth**
- 13 PCLinuxOS Recipe Corner: Skillet Coq Au Vin for Two**
- 14 PCLinuxOS Wiki Knowledgebase Resurrected!**
- 15 Screenshot Showcase**
- 16 New NIST Password Guidelines**
- 20 Screenshot Showcase**
- 21 How To Stop Advertisers From Tracking Your Teen
Across The Internet**
- 23 Salt Typhoon Hack Shows There's No Security Backdoor
That's Only For The "Good Guys"**
- 25 PCLinuxOS Recipe Corner Bonus:
Creamy Ground Beef Noodle Casserole**
- 26 Screenshot Showcase**
- 27 Exploring Typst: A LaTeX Alternative**
- 38 Screenshot Showcase**
- 39 GIMP Tutorial: Create A Double Exposure**
- 41 Tip Top Tips: Backing Up Your /home Directory**
- 42 Screenshot Showcase**
- 43 PCLinuxOS Puzzled Partitions**
- 47 More Screenshot Showcase**

The **PCLinuxOS** magazine

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

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

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)

Assistant Editor: Meemaw

Artwork: Paul Arnote, Meemaw

PDF Layout: Paul Arnote, Meemaw

HTML Layout: tbs, horusfalcon

Staff:

YouCanToo

David Pardue

Alessandro Ebersol

Contributors:

davecs

The PCLinuxOS Magazine is released under the Creative Commons Attribution-NonCommercial-Share-Alike 3.0 Unported license.

Some rights are reserved. Copyright © 2024.



From The Chief Editor's Desk

'Tis the season, I guess.

Everyone in our house has been sick and on antibiotics over the past month.

Except me.

It all started with Ryan being diagnosed with left lower lobe pneumonia. By the time he had finished up his first round of antibiotics, we had to go back to the urgent care clinic for more, because he definitely wasn't over it. They prescribed him another, more powerful antibiotic, which finally kicked the pneumonia to the curb.

At Ryan's second urgent care visit, Lexi also got seen because of a persistent cough and scratchy, irritated throat. The nurse practitioner said she had some rhinitis, and to treat it with antihistamines and decongestants. Two days later, we ended up right back at the urgent care clinic, because the rhinitis had precipitated a left ear infection. So, she ended up on a round of antibiotics as well to treat that.

Then, on the day that I returned from my deer hunting trip during the early antlerless firearm deer season, my wife went to the urgent care clinic. She was diagnosed with a right lower lobe pneumonia. They prescribed her an antibiotic, but when she was a few days into that round of antibiotics, it was evident that it wasn't the correct antibiotic. Fortunately, she ran into



No, Lexi's not taller than everyone. She is standing on a milk crate.

one of her favorite doctors while working at the hospital, who phoned a new prescription for a more appropriate antibiotic to our neighborhood pharmacy. Once that course of antibiotics was done, she still wasn't better, so off she went to the urgent care clinic, yet again. There, they "upgraded" her diagnosis to a persistent right lower lobe pneumonia, and ordered her on a third round of antibiotics. Finally, she is improving. Even as I write this, she is off for a followup visit at the urgent care clinic.

The physician she saw at her second urgent care clinic visit mentioned that the CDC has issued an advisory that atypical pneumonia diagnoses were on the rise across the country. Here's an [article](#) from the CDC that explains what has been going on, if you'd like to read more about it.

When we attended our kids' parent-teacher conferences, they mentioned that they had a lot of kids out with pneumonia. So, that is how

things have been in our home and area lately. To be perfectly honest, I have NO idea how I've escaped this onslaught unscathed. I've been surrounded by sickness, but have somehow evaded its grasp. How I've managed that feat, I don't know ... but I'm thankful.

So, be careful out there. Covid isn't our only pathogen/illness to worry about. This year's trivalent influenza vaccine has missed the mark on the prevalent strains going around (although it **will** convey some protection to you, and make the symptoms much milder should you be unfortunate enough to get an influenza infection ... so PLEASE go ahead and get your annual flu shot!). Now we also have to worry about this new atypical pneumonia going around.

Mother Nature must really have a burr in her knickers. Or, she really does hate us. I think the jury is still deliberating.

This month's cover was created by the Image Creator in Bing, powered by DALL-E-3 AI. It celebrates the International Space Station, which first "opened for business" on November 2, 2000. Linux users will be pleased to know that our favorite operating system occupies a key role in the day-to-day operations of the ISS. If

you're curious about the computers used aboard the ISS, you can "read more about it" from this [post](#) on Quora, by Robert Frost, Instructor and Flight Controller at NASA.

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



Screenshot Showcase



Posted by The CrankyZombie, on September 30, 2024, running KDE.



ICYMI: How To Tell If Someone Is Telling You The Truth

by Paul Arnote (parnote)



Image by [Temel](#) from [Pixabay](#)

Google employees' attempts to hide messages from investigators might backfire, according to an [article](#) at The Verge. The DOJ is trying to show that Google deliberately destroyed evidence that might have looked bad for it. Google employees liberally labeled their emails as “privileged and confidential” and spoke “off the record” over chat messages, even after being told to preserve their communications for investigators, lawyers for the Justice Department have told a Virginia court over the past couple of weeks. That strategy could backfire if the judge in Google’s second antitrust trial believes the company intentionally destroyed evidence that would have looked bad for it. The judge could go as far as giving an adverse inference about Google’s missing documents, which would mean assuming they would have been bad for Google’s case.

Google is misunderstood, its attorneys say in an antitrust trial, according to an [article](#) from Courthouse News Service. The Justice Department accuses the Silicon Valley tech firm of engaging in a systematic campaign to seize control of high-tech tools used by publishers, advertisers and brokers to facilitate digital advertising. Firing back against claims by the U.S. Justice Department that Google operates its ad business as a monopoly, a witness Monday described the mammoth search engine as acting in the best interests of publishers. “Innovation is at the heart of this business,” said Nitish Korula, a research scientist and engineering director for Google. “It’s a rapidly changing business. We keep looking for ways to make products better.” Korula described how the company walks publishers through the process of monetizing their websites and determining the kinds of ads appropriate for their brands. His testimony launched the third week of the antitrust trial before U.S. District Judge Leonie Brinkema, a Bill Clinton appointee. The Justice Department’s case, made in a [150-page complaint](#) filed in 2023, accuses the Silicon Valley tech firm of engaging in a systematic campaign to seize control of high-tech tools used by publishers, advertisers and brokers to facilitate digital advertising.

Two Play Store apps containing a malware Trojan that has affected over 11 million Android devices have been discovered, says an [article](#) from Lifehacker. The same malware was

also found in unofficial apps, which means the number of victims here is likely much higher. Researchers from Kaspersky [discovered](#) a new version of the Necro Trojan, which has attacked users from two sources: On the one hand, the Necro Trojan is being delivered through legitimate apps distributed on the Google Play Store. On the other, bad actors injected their Trojan into modified apps, such as custom versions of Spotify and Minecraft, that users downloaded through unofficial means—otherwise known as sideloading.



Image by [Rosy/Bad Homburg/Germany](#) from [Pixabay](#)

There are secrets from the CIA, FBI, and Special Forces on how to know if someone is telling the truth, and an [article](#) from Fast Company lays some of them out. CIA case officers and FBI agents say employing these techniques can help you make better decisions about how much you can trust another person.

Paying attention to body language is an essential component in the ongoing process of assessing a person's truthfulness. There's an often-used phrase: "What the mind conceals, the body reveals."

Google will soon start identifying when content in search and ad results is generated by AI — if you know where to look, according to an [article](#) from TechRepublic. In a Sep. 17 [blog post](#), the tech giant announced that, in the coming months, metadata in search, images, and ads will indicate whether an image was photographed with a camera, edited in Photoshop, or created with AI. Google joins other tech companies, including Adobe, in labeling AI-generated images.

From the "too little, too late" department, Microsoft's Secure Future Initiative was created around the same time the U.S. Cyber Safety Review Board chided Redmond for having a poor security culture. **On Sept. 23, Microsoft released a report detailing the progress of the Secure Future Initiative, the company-wide overhaul put in place in November 2023**, according to an [article](#) from TechRepublic. The Secure Future Initiative exists to improve security in the wake of some high-profile vulnerabilities in 2023. These vulnerabilities included a [breach](#) in Microsoft Exchange Online that allowed threat actors associated with the Chinese government to access U.S. government emails in 2023. In April 2024, the U.S. Cyber Safety Review Board published "Review of the Summer 2023 Microsoft Exchange Online Intrusion," which [said](#) the hack "was preventable and should never have occurred."

The board found Microsoft had "a corporate culture that deprioritized both enterprise security investments and rigorous risk management."



Mozilla

Mozilla has overhauled its branding to pay homage to its Netscape roots and better distinguish the wider organization from its Firefox web browser, according to an [article](#) from The Verge. The most notable change is to the company's logo: what was previously a sans-serif wordmark styled as "Moz://a" has been updated to correctly spell out the Mozilla name, featuring a new customized typeface and an M-shaped flag. According to Mozilla, the flag symbolizes the brand's "activist spirit." That fits with the image that the Mozilla Foundation, which is leading the company, is attempting to build: describing itself as "a non-profit organization that promotes openness, innovation, and participation on the Internet" and regularly releasing privacy reports that investigate tech companies' policy and security practices.

This month, Earth will grab itself a second moon in the form of the tiny asteroid 2024

PT5, according to an [article](#) from Space.com. Unlike the moon, Earth's primary companion which has accompanied our planet for around 4 billion years, this "new mini-moon" will stick around for just two months before it heads back to its home in an asteroid belt trailing our planet and orbiting the sun. It will be captured in Earth's gravitational pull between Sept. 29 and Nov. 25. Unfortunately, during its occupation around Earth, 2024 PT5 won't be visible to the vast majority of skywatchers. "The object is too small and dim for typical amateur telescopes and binoculars. However, the object is well within the brightness range of typical telescopes used by professional astronomers," research lead author and Universidad Complutense de Madrid professor Carlos de la Fuente Marcos said. "A telescope with a diameter of at least 30 inches plus a CCD or CMOS detector are needed to observe this object, a 30 inches telescope and a human eye behind it will not be enough." It could return this January, and astronomers predict it will return as a mini-moon in 2055 and again in 2084.

A Harvard medical student, Dr. Nick Norwitz, ate 720 eggs in a month to study the effects the "fowl" diet had on his cholesterol and saw that his levels dropped nearly 20 percent, according to an [article](#) from the New York Post. That averages out to one egg per hour over a 30-day period. Norwitz "hypothesized" before his experiment that consuming the 60 dozen eggs would not increase his LDL (low-density lipoprotein) or "bad" cholesterol by the time the month was over.



Image by [Gerd Altmann](#) from [Pixabay](#)

Do you remember that DNA sample you sent to 23 & Me? You have reason to be concerned. In late September 2024, all seven members of the board of directors resigned, effective immediately. That left CEO and founder Anne Wojcicki to navigate the downward spiral that the company's stock is in. Wojcicki wants to take the company private, mostly in response to the company's drastic drop in its stock price. The company has until November 4, 2024 to get the stock price back up over \$1 per share, or the company will be delisted from the stock exchange. It also remains a possibility that the company may be sold, along with the private and DNA data of its 15 million customers. The new owners may not see the protection of that private and DNA data to be as important as the company's founders do/does/did. This all comes on the heels of the company's \$30 million settlement with victims of a data breach in October 2023, where customer's private and DNA data were discovered on the dark web. Most of the customers targeted in the breach were of certain Chinese and Jewish descent. This information was gleaned from multiple news outlets. You can follow along [here](#) with this DuckDuckGo search.

In a recent study [published](#) in The Journal of Nutrition, **researchers in the United States analyzed data from the US NHANES study to evaluate the nutritional status of US adolescents and the impacts of added egg consumption on observed patterns.** Alarmingly, over 60% of adolescents were at risk of inadequacy in one or more of calcium, magnesium, choline, and essential vitamins ((e.g., vitamins D and E), potentially due to unhealthy eating behaviors (e.g., late-night snacks). Encouragingly, the consumption of primarily egg-based dishes was found to improve nutritional outcomes, with consumers exhibiting significantly higher choline, vitamin B2, vitamin D, selenium, lutein + zeaxanthin, docosahexaenoic acid, and protein levels than their egg-avoiding counterparts.

Drug repurposing — identifying new therapeutic uses for approved drugs — is often a serendipitous and opportunistic endeavor to expand the use of drugs for new diseases, according to a newly published [study](#) in Nature Medicine. The clinical utility of drug-repurposing artificial intelligence (AI) models remains limited because these models focus narrowly on diseases for which some drugs already exist. Here we introduce TxGNN, a graph foundation model for zero-shot drug repurposing, identifying therapeutic candidates even for diseases with limited treatment options or no existing drugs. Trained on a medical knowledge graph, TxGNN uses a graph neural network and metric learning module to rank drugs as potential indications and contraindications for 17,080 diseases. When benchmarked against 8 methods, TxGNN

improves prediction accuracy for indications by 49.2% and contraindications by 35.1% under stringent zero-shot evaluation. To facilitate model interpretation, TxGNN's Explainer module offers transparent insights into multi-hop medical knowledge paths that form TxGNN's predictive rationales. Human evaluation of TxGNN's Explainer showed that TxGNN's predictions and explanations perform encouragingly on multiple axes of performance beyond accuracy. Many of TxGNN's new predictions align well with off-label prescriptions that clinicians previously made in a large healthcare system. TxGNN's drug-repurposing predictions are accurate, consistent with off-label drug use, and can be investigated by human experts through multi-hop interpretable rationales.



*The PCLinuxOS Magazine
Created with Scribus*





Image by [Alexander Lesnitsky](#) from [Pixabay](#)

ChatGPT with GPT-4 uses approximately 519 milliliters of water, slightly more than one 16.9 ounce (500 ml) bottle, in order to write one 100-word email, according to original research from The Washington Post and the University of California, Riverside, says an article from TechRepublic. This extravagant resource use can worsen human-caused drought conditions, particularly in already dry climates. The Washington Post’s reporting is based on the research [paper](#) “Making AI Less “Thirsty”: Uncovering and Addressing the Secret Water Footprint of AI Models” by Mohammad A. Islam from UT Arlington, and Pengfei Li, Jianyi Yang, and Shaolei Ren of the University of California, Riverside. Reporters Pranshu Verma

and Shelly Tan and their editing team used public information for their calculations of water footprint estimates and electricity usage as detailed in their article. The Washington Post and the University of California, Riverside examined the electricity needed to run generative AI servers and the water to keep those servers cool. How much water and electricity are used in specific data centers can vary depending on the climate in which those data centers are located. Washington state and Arizona have particularly heavy water draws.

They’re burning the modern Library of Alexandria, asserts an [article](#) from Jacobin. That’s one way to describe the recent ruling of the Second Circuit US Court of Appeals against the Internet Archive (IA). The court sided with big-name publishers like Hachette, ruling that IA was violating copyright law with its online lending program. The [decision](#) nuked over five hundred thousand books from the IA lending library. The IA’s National Emergency Library (NEL) was a remarkable nonprofit initiative launched in 2020 during the pandemic, offering vital access to books while people were separated from their friends, family, colleagues, recreational sites, bookstores, and libraries. The separation affected leisure readers as well as those who rely on book access for work, including public and private researchers. The emergency library was part of the IA’s broader access program, the Open Library. The NEL, however, [allowed](#) more users to check out digital “copies” of books than they could under the more restricted Open Library rules. In essence, when the pandemic closed physical libraries, the IA threw open the doors of its

digital library. Knowledge, after all, wants to be free.

Despite a deluge in hardware news at Apple’s “It’s Glowtime” iPhone 16 event, Apple didn’t take any time to discuss repairability, according to an [article](#) from TechCrunch. It was a strange oversight, given the momentum that the right to repair movement has gained in recent years. A deeper dive after the event, however, has revealed several new iPhone 16 features designed to improve user access to device repair. The most interesting of the bunch is a new adhesive design that can be loosened by applying low voltage from a 9-volt battery. Glue has arguably been the biggest thorn in the side of DIY repairers. The thinner devices have become, the more manufacturers like Apple have grown dependent on the stuff in the place of screws.



NASA/JPL-Caltech

Currently, Voyager 1, launched September 5, 1977, is over 15 billion miles away, still communicating with Earth and providing valuable data from beyond the solar system’s boundary, says an [article](#) from ecotias.com. However, this unprecedented longevity comes

with challenges. The spacecraft's original design did not account for the extreme conditions it would face for decades. As a result, equipment degradation has been a persistent issue, possibly accelerated by space radiation. One significant problem was with the spacecraft's thrusters, crucial for maintaining its orientation and communication with Earth. Without functional thrusters, Voyager 1 would lose its ability to send data back to our planet. Among the numerous obstacles faced, the clogging of Voyager 1's thrusters has been particularly concerning. These thrusters are vital for keeping the spacecraft's High Gain Antenna pointed toward Earth, ensuring that it can receive commands and transmit data. The issue, caused by silicon dioxide buildup from the rubber diaphragm of the aging fuel tank, threatened to end the mission prematurely by compromising thrust generation and, consequently, orientation

control. To address this critical problem, NASA engineers needed to think creatively. You'll have to read the article to find out how NASA engineers managed to resolve the issue.

Microsoft's Digital Crimes Unit (DCU) is disrupting the technical infrastructure used by a persistent Russian nation-state actor Microsoft Threat Intelligence tracks as Star Blizzard, says an [article](#) from a Microsoft blog entry. Today, the United States District Court for the District of Columbia unsealed a civil action brought by Microsoft's DCU, including its order authorizing Microsoft to seize 66 unique domains used by Star Blizzard in cyberattacks targeting Microsoft customers globally, including throughout the United States. Between January 2023 and August 2024, Microsoft observed Star Blizzard target over 30 civil society organizations – journalists, think tanks, and non-governmental organizations (NGOs) core to ensuring democracy can thrive – by deploying spear-phishing campaigns to exfiltrate sensitive information and interfere in their activities.

In August, a threat actor compromised the data of 77,099 Fidelity Investments customers in Maine, the financial firm said in a breach notification letter to thousands of customers on Oct. 9, according to an [article](#) from TechRepublic. An attacker snuck in by creating two new user accounts. Fidelity assures customers their investments aren't affected. The attacker didn't access funds in Fidelity investment accounts. However, the hacker obtained personal information — including Social Security numbers and driver's licenses —

and created two new customer accounts. In response, Fidelity shut down the attacker's access and offered affected customers a credit monitoring and identity restoration service.



Mozilla, Firefox's developer, announced in a security advisory on October 9, 2024, that it had patched a "critical" flaw with the browser, according to an [article](#) from Lifehacker. The company says the issue, CVE-2024-9680, is a "use-after-free" flaw affecting Animation timelines. Use-after-free flaws occur when a system frees up memory, but a program continues to access it anyway. While this can result in general software issues, it also opens the door for bad actors to jump in. In this case, Mozilla confirms the flaw allows an attacker to "achieve code execution," or run their own malicious code, through the exploit. What makes this particular flaw a critical issue is that



it is a zero-day with an active exploit. A zero-day is a flaw discovered before the developer (Mozilla) has a chance to patch it. You can read Mozilla's announcement [here](#).

According to an [article](#) from The Verge, **The Internet Archive will come back within “days” following a cyberattack that brought down the organization’s vast digital library and the Wayback Machine**, says an [update](#) from founder Brewster Kahle. It's been struggling due to a [data breach and DDoS attack](#) during the first full week of October that revealed the email addresses, screen names, password change timestamps, and other information associated with more than 31 million unique email addresses. As of the time of this article's authorship (mid-October), The Internet Archive is back up.

Are you getting “app fatigue?” That's the issue that an [article](#) from The Atlantic takes a look at. These days, every Bob and his uncle seem to have their own dedicated mobile app. Do you want to take advantage of “in-app” only specials? You had better have the app installed. Do you want to get your food delivered? There's multiple apps for that, at least one for every service out there. Do you want to get your rewards from your favorite retailer? You had better use their app. Do you want to grab a ride from Uber or Lyft? There's an app for that (one for each service). If you have kids, there are probably more apps available to access school information for your kids than there are books in the schools (I personally have at least four different ones installed on my phone, as the school district keeps changing which ones they

choose to use). The proliferation of dedicated apps is frustrating, overwhelming and maddening.



Hackers are leveraging AI to hack your Gmail accounts, according to a [report](#) from Forbes. The attack is very sophisticated, and could fool even seasoned users. In fact, the attack is very convincing, and very scary. You will definitely want to read the entire article on this one, and pay particular attention to how the hack plays out at all levels. To be forewarned is to be forearmed.

Newly uncovered emails reveal how Google and Amazon used their access to the Office of the US Trade Representative as they sought to undermine overseas regulations — including efforts to protect traditional media outlets, according to an [article](#) from the New York Post. In May 2023, Google tried to enlist the USTR in its fight to defeat or at least water down Canada's Online News Act, which took effect last December. The law requires Google and Facebook parent Meta to pay publishers for the

right to display their content online. Meta exited Canada in response. That month, Google's head of trade policy Nicholas Bramble emailed three USTR staffers – senior director for services and digital trade Andrea Boron, deputy assistant trade representative Robb Tanner and director for Canada Randall Oliver – to request a meeting on “upcoming developments on Canada.”

Microsoft might be about to temporarily halt the rollout of its latest operating system update, Windows 11 24H2, for some users after reports of Blue Screen of Death (BSOD) errors emerged, according to an [article](#) from How-To-Geek. The issue appears to be linked to specific Western Digital SSDs and their interaction with the updated storage drivers in 24H2. The Windows 11 24H2 update includes



A magazine just isn't a magazine without articles to fill the pages. If you have article ideas, or if you would like to contribute articles to the

PCLinuxOS Magazine, send an email to:

[*pclinuxos.mag@gmail.com*](mailto:pclinuxos.mag@gmail.com)

We are interested in general articles about Linux, and (of course), articles specific to PCLinuxOS.

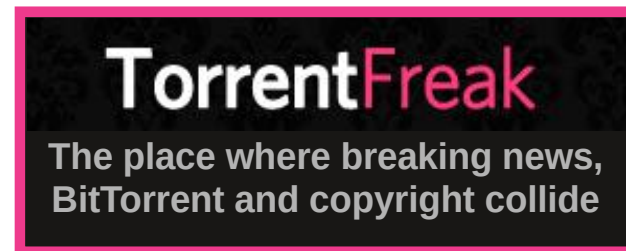
new File Explorer features, an updated Copilot experience, Wi-Fi 7 support, expanded availability for Voice Clarity audio, and much more.



The MX Linux forum has been under a botnet DDOS attack for several days, the MX Linux forum self-reported on October 14, 2024. It's not the biggest botnet around, but it's big enough to cause our server to struggle to keep up with the requests the bots are making. From what we can tell, the bots are just "clicking" on random forum links. As part of the defense, a Cloudflare captcha is being utilized to access the forum. Users may see that captcha even if they are not logging in. It's annoying, but this has been recommended at least as long as the attack is ongoing. Other steps, such as IP address blocking, are being taken as well.

The Federal Trade Commission announced on October 16, 2024, a final "click-to-cancel" rule that will require sellers to make it as easy for consumers to cancel their enrollment as it was to sign up. Most of the final rule's provisions will go into effect 180 days after it is published in the Federal Register. "Too often, businesses make people jump through endless hoops just to cancel a subscription," said Commission Chair Lina M. Khan. "The FTC's rule will end these tricks and traps, saving Americans time and money. Nobody should be stuck paying for a service they no longer want."

Google has gotten a bad reputation as of late for being a bit overzealous when it comes to fighting ad blockers, according to an article from Lifehacker. Most recently, it's been spotted automatically turning off popular ad blocking extension uBlock Origin for some Google Chrome users. To a degree, that makes sense—Google makes its money off ads. But with malicious ads and data trackers all over the internet these days, users have legitimate reasons to want to block them. The uBlock Origin controversy is just one facet of a debate that goes back years, and it's not isolated: your favorite ad blocker will likely be affected next. Here are the best ways to keep blocking ads now that Google is cracking down on ad blockers.



Last October, 23andme announced they had been attacked. A bad actor used a tactic called credential stuffing, where they were able to gain access to 23andme accounts by utilizing the users' credentials from their other compromised accounts, according to an article from Lifehacker. (As a side note, this highlights the importance of using a unique password for each of your accounts.) Through this credential stuffing, this actor was able to obtain information from DNA Relatives, as the feature relies on sharing data with other users you are genetically related to. That includes information like the user's display name, predicted relationships, and percentage of DNA that user shared with their matches. It also includes a number of optional data points if the user opted-in to sharing them, such as location, profile picture, birth year, and a link to their family tree. To that last point, a number of user data was compromised through the Family Tree feature.

According to an article from Bloomberg News, fentanyl is ridiculously cheap and roughly 100 times more potent than morphine. Mexican

cartels and other producers of illicit drugs add small amounts of it to cocaine, counterfeit versions of Adderall and other pills, methamphetamine and synthetic cannabis as an extremely cost-efficient filler that hooks customers. In slightly larger amounts — the equivalent of 10 to 15 grains of salt — it stops brain functions that regulate breathing. Fatal overdoses from fentanyl-laced drugs in the US and Canada have increased so rapidly over the past five years that some health officials classify it as an epidemic. Two years ago, JR Rahn had a thought: **What if you could treat fentanyl tragedies like you would a traditional health epidemic? Could you create a fentanyl vaccine?**

What was described as a “previously unknown” threat just three months ago has now prompted a third warning from the US government to update or stop using PCs, according to an [article](#) from Forbes. By exploiting old code buried under the covers of today’s Windows systems, it has quickly become clear that “a significant percentage of Windows devices are fully exposed and at risk of being taken over by attackers.” The latest vulnerability is CVE-2024-43573, which the [US cyber agency](#) warns is “an unspecified spoofing vulnerability which can lead to a loss of confidentiality.” It has mandated all federal employees to “apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable” by October 29. In other words, update your PC, or stop using it until you can.



Colossal, the de-extinction and species preservation company, announced numerous breakthrough successes in all stages of the thylacine de-extinction effort that put the company much closer to returning the iconic thylacine to Australia, says an [announcement](#) from the company. Thylacines (more commonly known as the Tasmanian Tiger), which have been extinct since 1936 due to human depredation, are a keystone species that is vital to the healthy function of the Tasmanian ecosystem, but are also an ideal candidate for the Colossal mission. Given their relatively recent extinction, many thylacine specimens are exceptionally well-preserved, allowing Colossal and its collaborators to push the boundaries of ancient DNA science and create the genomic blueprints for the thylacine’s return.

A typical large tree can suck as much as [40 kilograms](#) of carbon dioxide out of the air over the course of a year. **Now scientists at UC Berkeley say they can do the same job with less than half a pound of a fluffy yellow powder,** according to an [article](#) from the Los

Angeles Times. The powder was designed to trap the greenhouse gas in its microscopic pores, then release it when it’s ready to be squirreled away someplace where it can’t contribute to global warming. In tests, the material was still in fine form after 100 such cycles, according to a [study](#) published in the journal Nature.

Chemists at several universities, including the University of California, Riverside, looked at the process of photosynthesis, in which plants convert sunlight into the sugar they use to fuel their growth, and decided it may be too inefficient to keep up with the growing human demand for food, says an [article](#) from Gizmodo. In the journal [Joule](#), they wrote that **climate change and population growth are pushing humanity to develop better ways to grow crops that aren’t dependent on the Sun.** To that end, the team devised a new agricultural method, which they say bypasses conventional photosynthesis, and could be a part of the solution to the global problem of food insecurity.



Want to keep up on the latest that's going on with PCLinuxOS? Follow PCLinuxOS on Twitter!

<http://twitter.com/iluvpclinuxos>

PCLinuxOS Recipe Corner



Skillet Coq au Vin for Two

Serves 2

Special but still very much a down-home and hearty dish, Coq au Vin--chicken sautéed and then simmered in a rich red wine-and-mushroom sauce.

INGREDIENTS:

2 slices thick-cut bacon, chopped
1/2 cup frozen pearl onions, thawed
2 bone-in skin-on chicken thighs (about 3/4 lb)
1/4 teaspoon salt
1/4 teaspoon pepper
1/2 cup chopped onion
1 cup sliced mushrooms
1 clove garlic, finely chopped
1 tablespoon tomato paste
1/2 teaspoon finely chopped fresh thyme leaves
1 tablespoon all-purpose flour
1 cup dry red wine
1/2 cup chicken broth

1 tablespoon butter
1 tablespoon chopped fresh Italian
(flat-leaf) parsley

DIRECTIONS:

1. In a 10-inch skillet, cook bacon over medium heat for 4 to 6 minutes, stirring occasionally, until crisp. Using a slotted spoon, transfer bacon to a bowl. Add pearl onions to drippings in skillet; cook and stir for 1 to 2 minutes, or until browned. Transfer to another bowl.
2. Season chicken with salt and pepper. Place skin side down in skillet; cook over medium heat for 6 to 8 minutes, turning once, until browned on both sides. Remove from the skillet. Add onion and mushrooms to skillet; cook and stir for 4 to 5 minutes, or until lightly browned. Add garlic, tomato paste and thyme; cook and stir for 1 minute. Add flour; cook and stir for 1 minute.

3. Stir in red wine and broth; heat to boiling. Add the browned chicken and bacon, spooning some of the sauce over top of the chicken. Reduce heat to medium-low; cover and simmer for 20 to 25 minutes, turning chicken once halfway through, until juice of chicken is clear when thickest part is cut to bone (at least 165F). Stir browned pearl onions and butter into sauce; cook until heated through. Garnish with chopped parsley, and serve.

Expert Tips:

A dry red wine like Merlot or Cabernet Sauvignon works well in this recipe.

NUTRITION:

Calories: 523 Carbs: 18g Sodium: 651mg
Fiber: 3g Protein: 54g



PCLinuxOS Wiki Knowledgebase Resurrected!

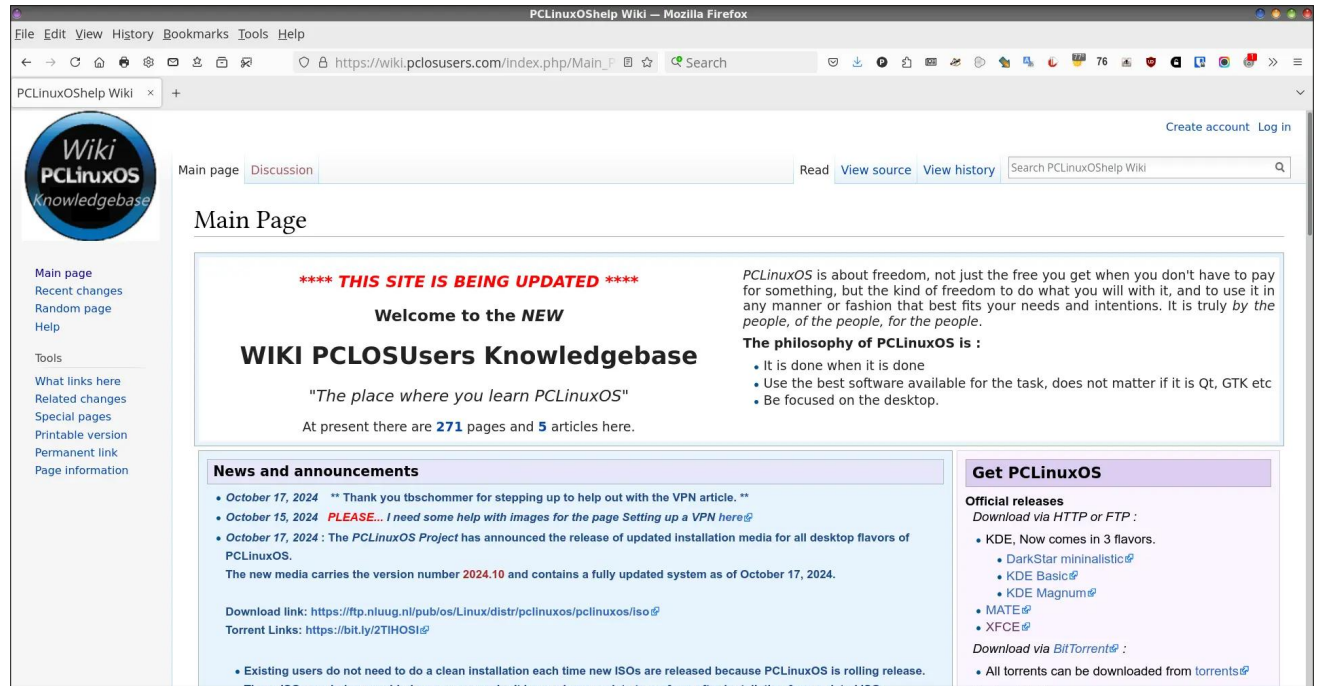
by Paul Arnote (parnote)

Thanks to the hard work of some incredible folks, the [PCLinuxOS Wiki Knowledgebase](#) has been resurrected!

Due to an unfortunate ransomware attack in mid-June, 2023, the “old” knowledgebase went down for the count. At the same time, the magazine’s website, PCLOS-Talk, the PCLinuxOS graphics site, and a few other sites PCLinuxOS users rely on also went down in the attack. You can read about it [here](#).

In the months after the ransomware attack, The CrankyZombie (upon whose servers those sites were running) tried several times to resurrect the knowledgebase, albeit unsuccessfully ... and through no fault of his. Many of the programs required to run some of the services had been updated since they were originally set up, and no longer ran on the server as they should.

The CrankyZombie, Meemaw and I worked tirelessly to restore the magazine’s website over the course of about three or four days. We were aided by an assortment of PCLinuxOS forum members, who helped supply missing files for the restoration that none of us had retained. Even today, 15 months later, I’m still finding random files that are missing (and I “fix” the problems as I find them). In the end, the biggest thing that is irretrievably missing are some



counter log files that log download numbers for the various versions of the magazine, as well as some page hits. If that’s all we lost, then I definitely consider the restoration efforts to have been a success.

Until the successful restoration of the wiki, the only access PCLinuxOS users had to the information contained in it was accessible via the Internet Archive’s [Wayback Machine](#). They had a copy of the wiki that dated back to 2022, so most of the site was intact. Only the changes/updates/new stuff since then were missing. It was the most complete copy of the “old” wiki available.

On October 4, 2024, I was contacted via PM by PCLinuxOS forum member CoreLite. He asked me whether I thought that there was enough interest in seeing the wiki resurrected. Of course, my answer was “DEFINITELY!” I added that while my plate was full, rendering me unable to assist much in the effort, I encouraged him to proceed with his attempt.

CoreLite managed to grab copies of as many of the “old” wiki pages from the Wayback Machine as he could (before they were hacked), and then proceeded to re-code all the links on the multitude of pages, removing the Wayback Machine’s redirection code.



Throughout the process, CoreLite would PM me to give me regular updates. Some users, like TerryN, had retained personal copies of the wiki pages that they had created. Others, like Kalwisti, forwarded his “manual” on the new installer. The “old” wiki URL had been taken over by a “URL Squatter,” and was unavailable. That necessitated a new domain name for the new wiki, which I linked to in the first paragraph of this article. The CrankyZombie is hosting the new wiki on his servers, as he had done the “old” wiki.

To say that the new wiki has been warmly received would be a gross understatement. Finally, PCLinuxOS users once again have a central location/site to share information covering hundreds of topics.

The Wiki Could Use Your Help

CoreLite was able to recover what’s estimated to be 90% of the old wiki.

With that in mind, there are “holes” in the knowledgebase to be filled. But that’s the nature of a wiki. Things change and evolve continuously.

If you have an area of expertise, no matter how small you think it is, please register and contribute articles to the new wiki. Posting how-to’s can help all PCLinuxOS users, old and new.

Wikis don’t typically use standard HTML for its articles. If you’re inclined to submit an article (or, even better, multiple articles) for the new

wiki, you will want to take a look at the syntax of the wiki markup language. It’s a simplified way of formatting text and other content. There is a guide to that wiki markup language on the PCLinuxOS Wiki, [here](#). If you want to take a deeper dive into using the wiki markup language, there’s a more comprehensive guide [here](#).

The most important thing to remember is that this is YOUR wiki. It doesn’t create itself. To be truly helpful and useful, PCLinuxOS users from all walks and expertise levels need to be

involved in creating and editing the articles it contains. The more people who participate, the better and more complete the information is ... and the more likely users will be able to find the information they are looking for.

PCLinuxOS users, unlike other Linux distros, frown on using the “RTFM” term that permeates other Linux distros. Having a good wiki provides the help users need to become productive, useful, helpful and satisfied users who will stay with PCLinuxOS for years to come.

Screenshot Showcase



Posted by tbs, on October 3, 2024, running KDE.

New NIST Password Guidelines

by Paul Arnote (parnote)



Image by [Gerd Altmann](#) from [Pixabay](#)

For what seems like an eternity, we've been urged, encouraged, prodded, poked, browbeat, pressured, reminded, cajoled, and any other word you can think of to create secure passwords. Part of that "programming" has included using a unique password for each login you have.

And, in a "more perfect world," that is great advice. But, once you start mixing in human failings, it all falls apart for a number of reasons. Probably one of the higher ranking problems with that advice is that most people cannot remember all of those different, unique passwords. The rigorous regimen for password creation, coupled with most people's inability to remember 100+ different passwords, has led to users committing the cardinal sin of reusing the same password on multiple sites. Once a password that has been reused on multiple sites

has been hacked, then all of the other accounts associated with that user where a password has been reused are also at risk.

The task is made even more difficult by previous password recommendations that forced users to have a mixture of upper and lower case letters, numbers and a non-alphanumeric symbol. Remembering even a dozen of those cryptic passwords is a task too difficult for most users.

I know we've covered password security ad-nauseum in the pages of The PCLinuxOS Magazine. I won't even attempt to count how many articles we've previously run, because my count of them varies each time I try. But trust me when I tell you that we've covered it a LOT. Couple that with virtually every other outlet in existence also harping on the same topic, and there's little to no doubt that you've received the "message," along with every other computer user on the planet. Whether that message was heeded, however, is a whole other matter.

Despite admonitions to the contrary, I'm certain that someone reading this has one of the following "passwords" to "secure" their private, personal data: passwOrd, password123, 12345678, 87654321, abc123, abcd1234, effthis, or one of MANY other insecure passwords that have been proven time and time again to be insecure. We've also run multiple articles on the annual "Worst Passwords of [YEAR]" in The PCLinuxOS Magazine. While

the list changes somewhat every year, many of the top 50 worst passwords on those lists remain stagnant and unchanged.



Image by [Temel](#) from [Pixabay](#)

Fortunately, the National Institute of Standards and Technology (NIST) may have just paved the road towards an easier life for computer users around the globe. They recently released a new set of updated [guidelines](#) for password generation and usage.

Actually, it's about time. The evidence for everything I just discussed has existed for several years now. We've even run multiple articles in the past detailing these new and improved regimens for password security. For what it's worth, NIST makes the



recommendations for cybersecurity for the U.S. government.

So, let's take a look at those NIST recommendations, and how you might be able to benefit.

When reading through these new password standards, keep in mind that those items labeled "SHALL" and "SHALL NOT" are requirements, while those labeled "SHOULD" and "SHOULD NOT" are strong recommendations. Whenever you come across the term "CSP," interpret that as "credential service provider," which can be a local credential service provider, or a third-party credential service provider. Even though NIST doesn't have any enforcement powers, their recommendations are typically enacted in toto.



Image by Christoph Meinersmann from Pixabay

Section 3.1.1.1: Password Authenticators

Passwords SHALL either be chosen by the subscriber, or assigned randomly by the CSP. If the CSP disallows a chosen password because it

is on a blacklist of commonly used, expected, or compromised values, the subscriber SHALL be required to choose a different password. Other complexity requirements for passwords SHALL NOT be imposed.

Section 3.1.1.2: Password Verifiers

There are nine key requirements under the new password recommendations.

First, passwords need to be a minimum of eight characters, with a minimum password length of 15 characters recommended.

Second, verifiers and CSPs also should allow passwords up to 64 characters in length.

Third, all ASCII printing characters, including the space character, should be allowed within the password.

Fourth, all Unicode characters should be accepted in passwords, and each Unicode character shall be counted as one character when evaluating password length.

Fifth, additional rules regarding password composition, such as a mixture of upper and lower case letters, numbers, and symbols, shall not be required for the composition of passwords.

It has been shown for quite some time that stringing together four or more common, random, unrelated words is at least as secure as requiring the mixture of characters, and it makes

remembering those passwords far, far easier for users to remember.

Sixth, there shall be NO requirement for users to periodically update their passwords, unless there is evidence that a user's password has become compromised.

Seventh, verifiers and CSPs shall not permit the subscriber to store a password hint that is accessible to an unverified claimant.

Eighth, subscribers shall not be prompted to use knowledge-based authentication (KBA) (e.g., "What was the name of your first pet?") or security questions when choosing passwords.

Ninth, verifiers shall verify the entire submitted password (i.e., not truncate it).



Image by S K from Pixabay

The recommendations continue beyond these nine requirements.

If Unicode characters are accepted in passwords, the verifier should apply the normalization process for stabilized strings using either the NFKC or NFKD normalization defined in Sec. 12.1 of Unicode Normalization Forms [UAX15]. This process is applied before hashing the byte string that represents the password. Subscribers choosing passwords that contain Unicode characters should be advised that some endpoints may represent some characters differently, which would affect their ability to authenticate successfully.

When processing a request to establish or change a password, verifiers shall compare the prospective password against a blocklist that contains known commonly used, expected, or compromised passwords. The entire password shall be subject to comparison, not substrings or words that might be contained therein. For example, the list may include, but is not limited to passwords obtained from previous breaches, dictionary words, and context-specific words, such as the name of the service, the username, and derivatives thereof.

If the chosen password is found on the blocklist, the CSP or verifier shall require the subscriber to select a different password and shall provide the reason for rejection. Since the blocklist is used to defend against brute-force attacks and unsuccessful attempts are rate-limited, the blocklist should be of sufficient size to prevent subscribers from choosing passwords

that attackers are likely to guess before reaching the attempt limit.

Verifiers shall offer guidance to the subscriber to assist the user in choosing a strong password. This is particularly important following the rejection of a password on the blocklist as it discourages trivial modification of listed weak passwords [Blocklists].

Verifiers shall implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account.



Image by Pokomon from Pixabay

Verifiers shall allow the use of password managers. Verifiers should permit claimants to use the “paste” functionality when entering a password to facilitate their use. Password managers have been shown to increase the likelihood that users will choose stronger passwords, particularly if the password managers include password generators. [Managers].

Users on PCLinuxOS can use multiple password managers to help remember the vast quantity of passwords. One that I use quite regularly is

Bitwarden, which we covered previously in The PCLinuxOS Magazine, [here](#) and [here](#). I’ve also used **KeepassX** in the past, which we’ve covered [here](#) and [here](#).

To assist the user in successfully entering a password, the verifier should offer an option to display the secret — rather than a series of dots or asterisks — while it is entered and until it is submitted to the verifier. This allows the claimant to confirm their entry if they are in a location where their screen is unlikely to be observed. The verifier may also permit the user’s device to display individual entered characters for a short time after each character is typed to verify the correct entry. This is common on mobile devices.

Verifiers may make allowances for mistyping, such as removing leading and trailing whitespace characters before verification or allowing the verification of passwords with differing cases for the leading character, provided that passwords remain at least the required minimum length after such processing.



Verifiers and CSPs shall use approved encryption and an authenticated protected channel when requesting passwords.



Image by [Gerd Altmann](#) from [Pixabay](#)

Verifiers shall store passwords in a form that is resistant to offline attacks. Passwords shall be salted and hashed using a suitable password hashing scheme. Password hashing schemes take a password, a salt, and a cost factor as inputs and generate a password hash. Their purpose is to make each password guess more expensive for an attacker who has obtained a hashed password file, thereby making the cost of a guessing attack high or prohibitive. The chosen cost factor should be as high as practical without negatively impacting verifier performance. It should be increased over time to account for increases in computing performance. An approved password hashing scheme published in the latest revision of [SP800-132] or updated NIST guidelines on password hashing schemes should be used. The chosen output length of the password verifier, excluding the salt and versioning information, should be

the same as the length of the underlying password hashing scheme output.

The salt shall be at least 32 bits in length and chosen to minimize salt value collisions among stored hashes. Both the salt value and the resulting hash shall be stored for each password. A reference to the password hashing scheme used, including the work factor, should be stored for each password to allow migration to new algorithms and work factors. For example, for the Password-Based Key Derivation Function 2 (PBKDF2) [SP800-132], the cost factor is an iteration count: the more times that the PBKDF2 function is iterated, the longer it takes to compute the password hash.

In addition, verifiers should perform an additional iteration of a keyed hashing or encryption operation using a secret key known only to the verifier. If used, this key value shall be generated by an approved random bit generator. The secret key value shall be stored separately from the hashed passwords. It should be stored and used within a hardware-protected area, such as a hardware security module or trusted execution environment (TEE). With this additional iteration, brute-force attacks on the hashed passwords are impractical as long as the secret key value remains secret.

But Wait ... There's More!

The new NIST guidelines also continue on to [cover](#) "Look-Up Secrets," and how CSPs should handle those types of requests. They also offer

updated [guidance](#) on how to handle multifactor authentication.

I'll leave looking up the information for those methodologies as something for you to do on your own. I'll also urge you to view the rationale for these changes by cross-referencing with the article's [Appendix](#), which does a decent job of explaining the reason for the changes.

Summary

The new NIST guidelines for passwords are long, long overdue, seeing how the information supporting these changes has been around for at least five years. Anything that can make remembering passwords easier will also make it easier for users to NOT reuse passwords on multiple sites. And, as you can see, these changes are quite wide in their scope and breadth.

This is, without any argument, a HUGE step in the right direction. As huge as these changes are, don't hold your breath waiting for the recommendations to be adopted quickly and en masse. There will be resistance, as well as those who are unaware of the changes brought forth in the new recommendations. Some people absolutely hate change, in any shape, form, or color. It will take some time, so don't expect to see these changes happen overnight. Some CSPs and verifiers will try to claim that the current password regimen is not broken, and will resist to the nth degree. Except, the current system is broken, as evidenced by users taking the

shortcut of reusing passwords for multiple logins.

If you want to read more about these new password recommendations (besides the NIST document itself, which is rather dry reading material), I can recommend these two sites to start your dive into these changes. The first one is an [article](#) from Intelligent Technical Solutions. The other [article](#) is from Specops Software. Both have great information on the recommended password regimen changes.

Creating a unique and secure password is YOUR responsibility. No one else is going to protect it for you. No one else has as much vested interest in protecting your private, personal data as you do. These changes should help keep your private, personal data safe from prying eyes, but only if you follow these recommendations.



PCLOS-Talk
Instant Messaging Server
Sign up TODAY! <http://pclostalk.pclosusers.com>

Instant Messages

Screenshot Showcase



Posted by parnote, on October 9, 2024, running Xfce.



How To Stop Advertisers From Tracking Your Teen Across The Internet

by Guest Author and [Erica Portnoy](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons License

This post was written by EFF fellow Miranda McClellan.

Teens between the ages of 13 and 17 are being tracked across the internet using identifiers known as Advertising IDs. When children turn 13, they age out of the data protections provided by the Children's Online Privacy Protection Act (COPPA). Then, they become targets for [data collection](#) from data brokers that collect their information from social media apps, shopping history, location tracking services, and more. Data brokers then process and sell the data. [Deleting](#) Advertising IDs off your teen's devices can increase their privacy and stop advertisers collecting their data.

What is an Advertising ID?

[Advertising identifiers](#) – Android's Advertising ID (AAID) and Identifier for Advertising (IDFA) on iOS – enable third-party advertising by providing device and activity tracking information to advertisers. The advertising ID is a string of letters and numbers that uniquely identifies your phone, tablet, or other smart device.



How Teens Are Left Vulnerable

In most countries, children must be [over 13 years old](#) to manage their own Google account without a supervisory parent account through Google Family Link. Children over 13 gain the right to manage their own account and app downloads without a supervisory parent account — and they also gain an Advertising ID.

At 13, children transition abruptly between two extremes — from potential helicopter parental surveillance to surveillance advertising that connects their online activity and search history to marketers serving targeted ads.

Thirteen is a historically significant age. In the United States, both [Facebook](#) and [Instagram](#) require users to be at least 13 years old to make an account, though many children [pretend](#) to be older. The Children's Online Privacy Protection Act (COPPA), a federal law, requires companies to obtain "[verifiable parental consent](#)" before collecting personal information from children under 13 for commercial purposes.

But this means that teens can lose valuable privacy protections even before becoming adults.



commandlinefu.com

How To Stop Advertisers From Tracking Your Teen Across The Internet

How to Protect Children and Teens from Tracking

Here are a few steps we recommend that protect children and teens from behavioral tracking and other privacy-invasive advertising techniques:

- Delete advertising IDs for minors aged 13-17.
- Require schools using Chromebooks, Android tablets, or iPads to educate students and parents about deleting advertising IDs off school devices and accounts to preserve student privacy.
- Advocate for extended privacy protections for everyone.

How to Delete Advertising IDs

Advertising IDs track devices and activity from connected accounts. Both Android and iOS users can reset or delete their advertising IDs from the device. Removing the advertising ID removes a key component advertisers use to identify audiences for targeted ad delivery. While users will still see ads after resetting or deleting their advertising ID, the ads will be severed from previous online behaviors and provide less personally targeted ads.

Follow these instructions, updated from a previous [EFF blog post](#):

On Android

With the release of [Android 12](#), Google began allowing users to delete their ad ID permanently.

On devices that have this feature enabled, you can open the **Settings** app and navigate to **Security & Privacy > Privacy > Ads**. Tap **“Delete advertising ID,”** then tap it again on the next page to confirm. This will prevent any app on your phone from accessing it in the future.

The Android opt out should be available to most users on Android 12, but may not be available on older versions. If you don't see an option to "delete" your ad ID, you can use the older version of Android's privacy controls to reset it and ask apps not to track you.

On iOS

Apple requires apps to [ask permission](#) before they can access your IDFA. When you install a new app, it may ask you for permission to track you.

Select **“Ask App Not to Track”** to deny it IDFA access.

To see which apps you have previously granted access to, go to **Settings > Privacy & Security > Tracking**.

In this menu, you can disable tracking for individual apps that have previously received permission. Only apps that have permission to track you will be able to access your IDFA.

You can set the **“Allow apps to Request to Track”** switch to the **“off”** position (the slider is to the left and the background is gray). This will prevent apps from asking to track in the future. If you have granted apps permission to track you

in the past, this will prompt you to ask those apps to stop tracking as well. You also have the option to grant or revoke tracking access on a per-app basis.

Apple has its own targeted advertising system, separate from the third-party tracking it enables with IDFA. To disable it, navigate to **Settings > Privacy > Apple Advertising** and set the **“Personalized Ads”** switch to the **“off”** position to disable Apple's ad targeting.

Miranda McClellan served as a summer fellow at EFF on the Public Interest Technology team. Miranda has a B.S. and M.Eng. in Computer Science from MIT. Before joining EFF, Miranda completed a Fulbright research fellowship in Spain to apply machine learning to 5G networks, worked as a data scientist at Microsoft where she built machine learning models to detect malware, and was a fellow at the Internet Society. In her free time, Miranda enjoys running, hiking, and crochet.

At EFF, Miranda conducted research focused on understanding the data broker ecosystem and enhancing children's privacy. She received funding from the National Science Policy Network.

**Looking for an old article?
Can't find what you want?**

**Try the PCLinuxOS Magazine's
searchable index!**

The **PCLinuxOS** magazine

Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys"

by [Joe Mullin](#) and [Cindy Cohn](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons License

At EFF, we've long noted that you cannot build a backdoor that only [lets in good guys](#) and not bad guys. Over the weekend, we saw another example of this: The Wall Street Journal [reported](#) on a major breach of U.S. telecom systems attributed to a sophisticated Chinese-government backed hacking group dubbed Salt Typhoon.

According to reports, the hack took advantage of systems built by ISPs like Verizon, AT&T, and Lumen Technologies (formerly CenturyLink) to give law enforcement and intelligence agencies access to the ISPs' user data. This gave China unprecedented access to [data](#) related to U.S. government requests to these major telecommunications companies. It's still unclear how much communication and internet traffic, and related to whom, Salt Typhoon accessed.

That's right: the path for law enforcement access set up by these companies was apparently compromised and used by China-backed hackers. That path was likely created to facilitate smooth compliance with wrong-headed laws like [CALEA](#), which require telecommunications companies to facilitate "lawful intercepts" — in other words, wiretaps and other orders by law enforcement and national security agencies.



While this is a terrible outcome for user privacy, and for U.S. government intelligence and law enforcement, it is not surprising.

The idea that only authorized government agencies would ever use these channels for acquiring user data was always risky and flawed. We've seen this before: in a notorious case in 2004 and 2005, more than 100 top officials in the Greek government were [illegally surveilled](#) for a period of ten months when unknown parties broke into Greece's "lawful access" program. In 2024, with growing numbers of sophisticated state-sponsored hacking groups operating, it's almost inevitable that these types of damaging breaches occur. The system of

special law enforcement access that was set up for the "good guys" isn't making us safer; it's a dangerous security flaw.

Internet Wiretaps Have Always Been A Bad Idea

Passed in 1994, [CALEA](#) requires that makers of telecommunications equipment provide the ability for government eavesdropping. In 2004, the government dramatically expanded this wiretap mandate to include internet access providers. EFF [opposed](#) this expansion and explained the perils of wiretapping the internet.

Salt Typhoon Hack Shows There's No Security Backdoor That's Only For The "Good Guys"

The internet is different from the phone system in critical ways, making it more vulnerable. The internet is open and ever-changing. “Many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more pregnable to attackers who want to steal their data or personal information,” EFF wrote, nearly 20 years ago.

Towards Transparency And Security

The irony should be lost on no one that now the Chinese government may be in possession of more knowledge about whom the U.S. government spies on, including people living in the U.S., than Americans. The intelligence and law enforcement agencies that use these backdoor legal authorities are notoriously secretive, making oversight difficult.

Companies and people who are building communication tools should be aware of these flaws and implement, where possible, [privacy by default](#). As bad as this hack was, it could have been much worse if it wasn't for the hard work of EFF and other privacy advocates making sure that more than 90% of web traffic is encrypted via HTTPS. For those hosting the 10% (or so) of the web that has yet to encrypt its traffic, now is a great time to consider turning on encryption, either using [Certbot](#) or switching to a [hosting provider](#) that offers HTTPS by default.

What can we do next? We must demand real privacy and security.

That means we must reject the loud law enforcement and other voices that continue to pretend that there are “good guy only” ways to ensure access. We can point to this example, among many others, to push back on the idea that the default in the digital world is that governments (and malicious hackers) should be able to access all of our messages and files. We'll continue to fight against US bills like [EARN IT](#), the [EU “Chat Control”](#) file-scanning proposal, and the [UK's Online Safety Act](#), all of which are based on this flawed premise.

It's time for U.S. policymakers to step up, too. If they care about China and other foreign countries engaging in espionage on U.S. citizens, it's time to speak up in favor of [encryption by default](#). If they don't want to see bad actors take advantage of their constituents, domestic companies, or security agencies, again — speak up for encryption by default. Elected officials [can and have](#) done so in the past. Instead of holding hearings that give the FBI a platform to make digital wiretaps easier, demand accountability for the digital lock-breaking [they're already doing](#).

The lesson will be repeated until it is learned: there is no backdoor that only lets in good guys and keeps out bad guys. It's time for all of us to recognize this, and take steps to ensure real security and privacy for all of us.



PCLinuxOS Recipe Corner Bonus



Creamy Ground Beef Noodle Casserole

Serves: 6

INGREDIENTS:

8 oz uncooked Farfalle pasta (about 2 1/2 cups)
1 lb ground beef
1 can (15 oz) tomato sauce
1/2 teaspoon garlic salt
1/4 teaspoon black pepper
1 cup sour cream
1 cup cottage cheese
1/2 cup shredded Parmesan cheese
3/4 cup sliced green onions
1 1/2 cups shredded Cheddar cheese (12 oz)

DIRECTIONS:

1. Heat oven to 350°F. Spray a 13x9-inch baking dish or 2 1/2 to 3-quart casserole with cooking spray. Cook pasta until al dente, about 11 minutes; drain, and set aside.

2. Meanwhile, in a 10-inch nonstick skillet, cook beef over medium-high heat 5 to 7 minutes, stirring frequently, until no longer pink; drain. Stir in tomato sauce, garlic salt and pepper; cover and simmer for 2 to 3 minutes or until slightly thickened.

3. In a large bowl, mix sour cream, cottage cheese, Parmesan cheese and 1/2 cup of the green onions; stir in cooked pasta.

4. Spoon half of the pasta mixture into a baking dish. Top with half of the beef mixture and 3/4 cup of the Cheddar cheese. Repeat with pasta mixture, beef mixture and remaining 3/4 cup Cheddar cheese. Bake uncovered 25 to 30 minutes, or until mixture is thoroughly heated and cheese is melted. Top with remaining 1/4 cup green onions, and serve.

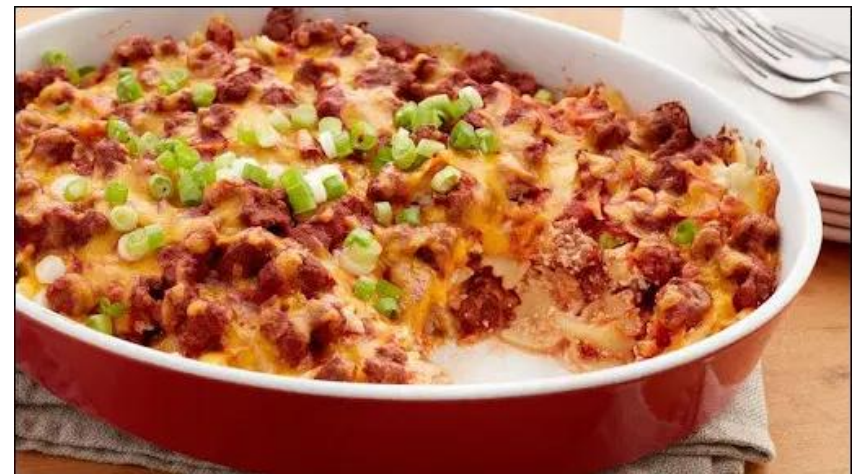
TIPS:

Wide egg noodles or Mafalda pasta would also work in this recipe.

Stir 1/2 teaspoon crushed red pepper into beef mixture for a spicy kick.

NUTRITION:

Calories: 580 Carbs: 43g Fiber: 3g
Sodium: 1010mg Protein: 35g



Disclaimer

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

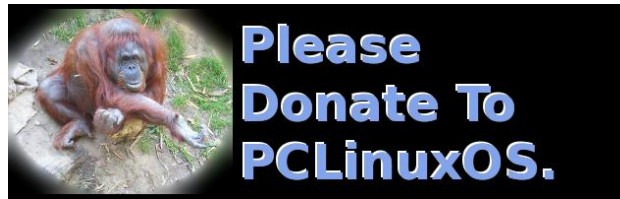
2. The information in the PCLinuxOS Magazine is provided on an "AS IS" basis, and all warranties, expressed or implied of any kind, regarding any matter pertaining to any information, advice or replies are disclaimed and excluded.

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

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

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

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



Screenshot Showcase



Posted by mutse, on October 5, 2024, running Mate.

Exploring Typst: A LaTeX Alternative

by David Pardue (kalwisti)

Although my educational background is not in STEM, I have been using LaTeX for approximately seventeen years. I am a fan of its typesetting capabilities but try not to be a LaTeX evangelist — or a LaTeX snob. I keep an open mind towards possible alternatives; I have dabbled with the [LyX](#) document processor (which uses LaTeX as its typesetting engine) as well as the [GNU TeXmacs](#) scientific editor (not based on LaTeX but inspired by it). I am aware of the [SILE](#) typesetter (which contains a port of the TeX line-breaking algorithm) as well as the old-school [groff](#) (also known as GNU roff) typesetting system. To date, I have not yet experimented with either SILE or groff.

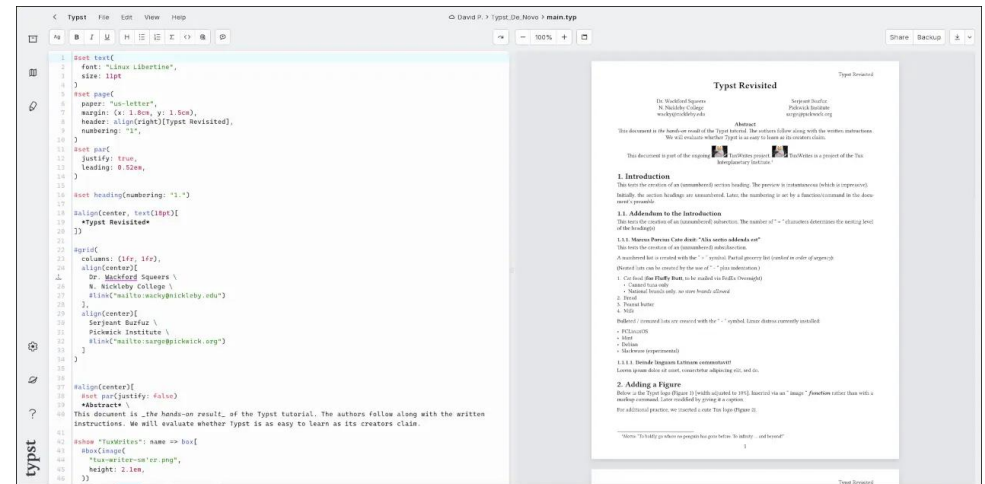


A newcomer on the scene is Typst (IPA: /tarpst/, "Ty" like in Typesetting and "pst" like in Hipster). It is a markup-based typesetting system that is designed to be as powerful as LaTeX, while claiming to be much easier to learn and use. I was hesitant to try Typst because I was not sure how much LaTeX I would have to unlearn in order to acquire a basic knowledge of Typst. However, after reading many positive comments about the application, I became convinced to dive in. In this article, I will provide an overview of Typst and describe my experience with it from the perspective of an (intermediate-level) LaTeX user.

I should mention that Typst is not currently in the PCLinuxOS repositories. It is possible to install the Typst compiler and its CLI locally; I will cover that procedure in next month's article. In the meantime, the most comfortable way of using Typst is to sign up for its online app at <https://typst.app/>. It furnishes an integrated IDE-like experience with autocompletion, syntax highlighting and instant preview. Another

advantage of the web app is that you do not need to install anything on your computer.

Typst has adopted a freemium [pricing](#) model; their Free plan offers basic features (enough to use it productively) while the Pro plan provides extra functionality and storage for a subscription fee (\$7.99 US per month or \$79.99 US per year).



Origins of Typst

Typst was created by two computer science graduates: Martin Haug and Laurenz Mädje. They began developing Typst in 2019, due to their frustrations with LaTeX. Typst started as a hobby project, but it has since grown into a full-fledged typesetting system. Haug and Mädje founded the startup Typst company in 2023, with headquarters in Berlin. Haug presents Typst's history in more detail, in his [talk](#) "LaTeX: It's Not You, It's Me" (presented at the Ubuntu Summit [Nov. 2023, Riga, Latvia]). Mädje wrote his Master's [thesis](#), "Typst: A Programmable Markup Language for Typesetting" (2022), using the new Typst software. Haug also wrote his



Master's [thesis](#), "Fast Typesetting with Incremental Compilation" (2022), on the topic of Typst.

Typst is funded by the Technical University of Berlin [Technische Universität Berlin], the State of Berlin and the European Union (through the European Social Funds).

Typst is not a wrapper around TeX, nor is it a "better implementation" of LaTeX. It is written in Rust and is a completely different software. Typst is open-source, with the [compiler](#) and CLI available on GitHub under an Apache 2.0 license. The libraries created for Typst, such as [svg2pdf](#), [biblatex](#), and [pdf-writer](#) are also open source.

It is important to remember that Typst is a work in progress, under rapid development. (In fact, Typst was just updated to ver. 0.12.0 while I was preparing this article.) Although the developers have been very responsive to user feedback, Typst lacks the complete, rich feature set of LaTeX and its package ecosystem lags far behind that of TeX and friends. Nevertheless, considering how young Typst is, my experience with it was positive.

Advantages over LaTeX

Typst claims to have several advantages over LaTeX, such as:

Intuitive and easy to learn. I believe the easiest way to get started with Typst is to register for the free web app and work through the four-chapter online [tutorial](#). I estimate that, working slowly, it took me approximately two hours to complete.

If you're already familiar with LaTeX, there is a Typst quick-start "[Guide for LaTeX Users](#)" which explains the main differences between these two typesetting systems.

Once you have acquired the basics, you can consult Typst's thorough online [documentation](#) for reference. Help is also available via Discord or the recently created [user forum](#).

Although there is a learning curve with Typst, my impression thus far is that it is less steep than learning LaTeX (which one Reddit commenter succinctly described as "high-effort/high-reward").

Typst's live, incremental compilation allows you to preview your changes instantly. Based on my experience, this claim is accurate. Typst compiles faster than LaTeX; compilation typically takes milliseconds rather than seconds.

Typst provides clear, understandable error messages. This claim is also true. Although I enjoy using LaTeX, I admit that error messages are one of its "pain points." Users quickly become familiar with [common error messages](#), but non-trivial errors can be difficult to interpret. (If I had a nickel for every LaTeX error that I have generated over the years, I would be a multimillionaire!)

As a small example, let us compare a simple/common LaTeX error message (taken from within my [Overleaf](#) account) to a Typst error message.

In the screenshot below, I intentionally omitted the closing square bracket of the item in LaTeX's description environment. (It should be "`\item[YAML] "`):

```
475 \section{Intentional Mistakes \& Error Messages}
476
477 \begin{description}
478   \item[YAML] "YAML Ain't a Markup Language"
479 \end{description}
480
481 \end{document}
```

Overleaf's editor alerts me that there is a problem by displaying a red circle in the left margin. When I view the log file, I see this:

```
Runaway argument?
main.tex, 480

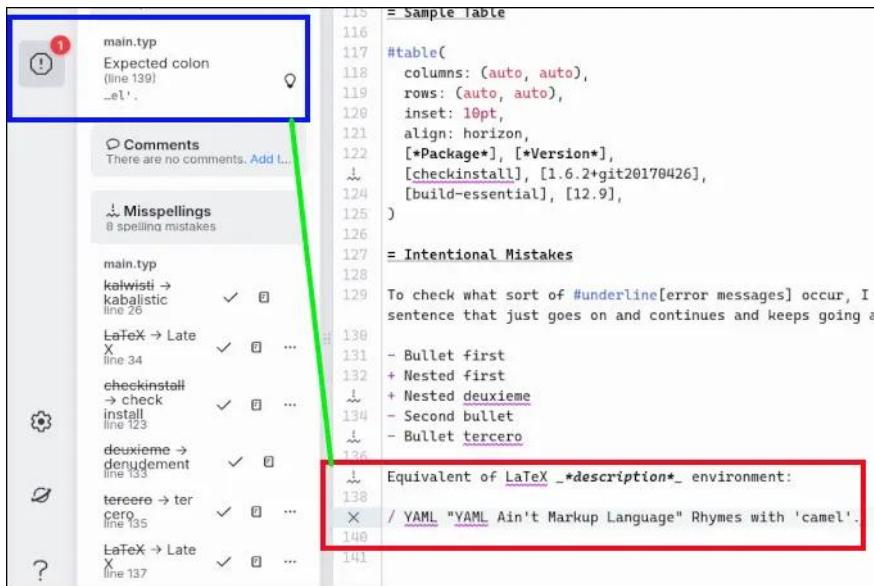
YAML "YAML Ain't a Markup Language" \end {description}
! Paragraph ended before \@item was complete.
<to be read again>
\par
l.480

I suspect you've forgotten a `}', causing me to apply this
control sequence to too much text. How can we recover?
My plan is to forget the whole thing and hope for the best.
```

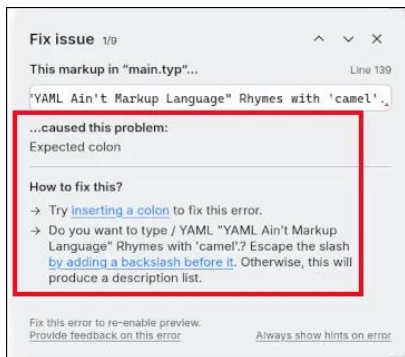
LaTeX categorizes the error as a "Runaway argument?" and states that the "\@item " is incomplete but does not suggest how I can fix it.

Typst's error messages try to guide you towards a solution. In the screenshot below, while experimenting with the `term list` function, I intentionally omitted the mandatory colon following the term. (It should be "/ YAML: ")

Typst not only notifies me of the error, but also helpfully suggests that a colon is expected in this environment:



There is also a pop-up dialog that appears in the web app's interface:



Typst has a consistent styling system for configuring everything from fonts and margins to the appearance of headings and lists. Also, Typst uses familiar programming constructs instead of hard-to-understand macros. Functions are written in a nice, JavaScript-like programming language.

For bibliography and reference management, Typst uses either the new bibliography file format called Hayagriva (which has the extension .yml), or a traditional BibLaTeX .bib file. The Hayagriva YAML file format is described [here](#). (I did not have enough time to experiment with Hayagriva, but I used a sample .bib file, which worked fine.)

A Glimpse at Typst's Structure

A complete description of Typst's structure is beyond the scope of this introductory article. As a non-programmer, I also lack in-depth knowledge to understand all of Typst's programming concepts. Therefore, I will try to offer only a glimpse at a few characteristics of the system.

Like LaTeX, Typst is a markup-based typesetting system. You compose your document in a text file and mark it up with commands and other syntax. Then, you use a compiler to typeset the source file into a PDF.

However, Typst's creators made design decisions which differ from LaTeX. For instance, Typst uses markdown syntax instead of commands for common tasks. To italicize a word or phrase, Typst uses single underscores (as shown below):

`_lorem ipsum_` produces the output *lorem ipsum*

Whereas LaTeX uses this command:

`\textit{lorem ipsum}` produces the output *lorem ipsum*

To boldface a word or phrase:

Typst: `*dolor sit*` produces the output **dolor sit**

LaTeX: `\textbf{dolor sit}` produces the output **dolor sit**

LaTeX has 'environments' to create different sorts of lists: `itemize` (for bulleted lists), `enumerate` (for numbered/ordered lists), and `description` (for lists labeling each entry item). In contrast, Typst uses markdown (as shown below for a bulleted/itemized list):

<pre>To write this list in Typst... '''latex \begin{itemize} \item Fast \item Flexible \item Intuitive \end{itemize} ...just type this: - Fast - Flexible - Intuitive</pre>	<pre>To write this list in Typst... \begin{itemize} \item Fast \item Flexible \item Intuitive \end{itemize} ...just type this: • Fast • Flexible • Intuitive</pre>
--	---

For a numbered list, Typst uses a plus symbol (+) rather than LaTeX's `enumerate` environment:


- + Fast
- + Flexible
- + Intuitive

Typst differentiates between markup mode and code mode. The default is markup mode, where you compose text and apply syntactic constructs such as ***asterisks for bold text***. Code mode, on the other hand, parallels programming languages like Python, providing the option to input and execute segments of code.

Within Typst's markup, you can switch to code mode for a single command (or rather, expression) using a hash (#). This is how you call functions to, for example, split your project into different files or render text based on some condition, e.g., Let me show how to do

`#underline([_underlined_ text])` produces Let me show how to do underlined text.

Typst has functions that *insert* content (for example, the `image` function shown below):



<pre>#figure(image("molecular.jpg", width: 80%), caption: [A step in the molecular testing pipeline of our lab.],)</pre>	 <p>Figure 1: A step in the molecular testing pipeline of our lab.</p>
--	---

while other functions *manipulate* content that they receive as arguments (e.g., the `align` function):

<pre>#set align(center) Centered text, a sight to see \ In perfect balance, visually \ Not left nor right, it stands alone \ A work of art, a visual throne</pre>	<p>Centered text, a sight to see In perfect balance, visually Not left nor right, it stands alone A work of art, a visual throne</p>
--	---

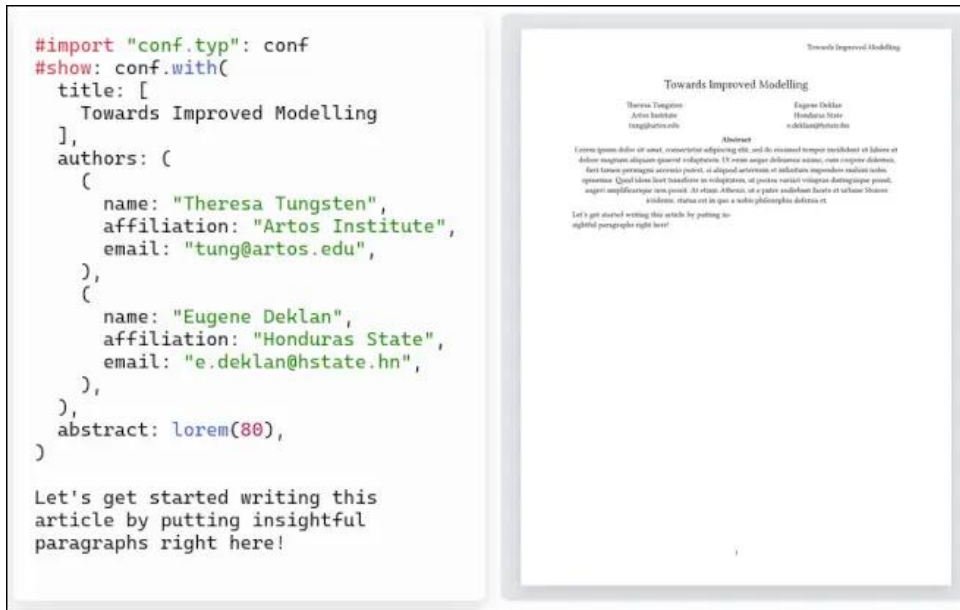
Typst's online documentation includes a full syntax cheat sheet, available at <https://typst.app/docs/reference/syntax/>.

Another significant difference between the typesetting systems is that LaTeX uses different document classes (`article`, `report`, `book`, `letter`, etc.) to define how your document is supposed to look, whereas Typst styles your document via functions. Typically, you use a template that provides a function that styles your whole document. First, you import the function from a template file. Then, you apply it to your whole document. This is accomplished with a 'show rule' that wraps the following document in a given function. The following example illustrates how it works (next page, top left):

	<p>Like Us On Facebook! The PCLinuxOS Magazine PCLinuxOS Fan Club</p>	
---	---	---

Dashboard

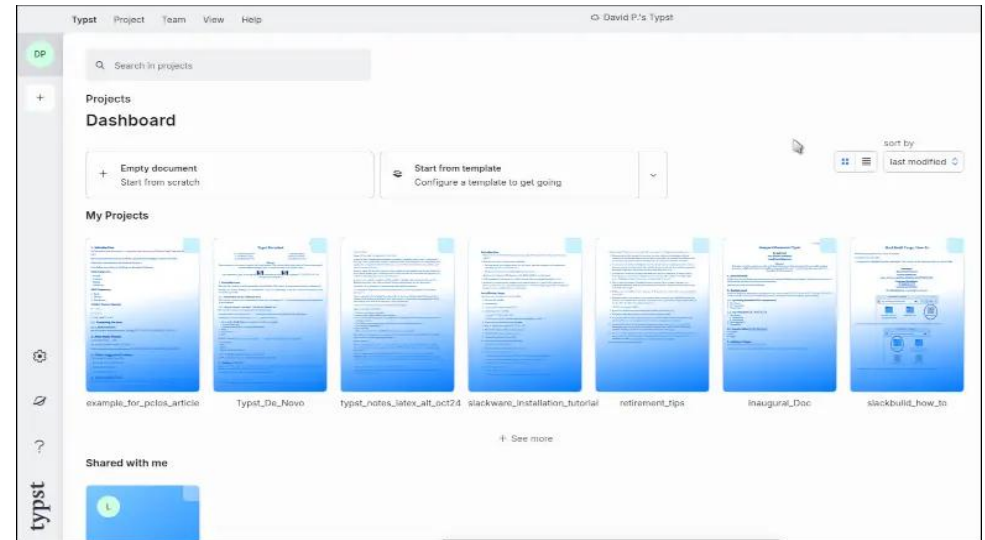
After logging in to the web app, you will land in the Dashboard area, which displays thumbnails of your Typst projects:



Typst's Web App

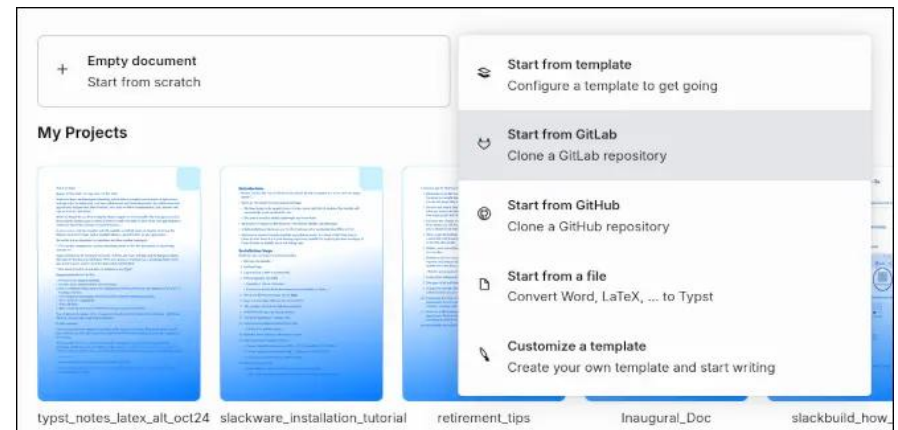
Although the Typst compiler (its core typesetting engine) is open-source, the web app is proprietary and closed-source. Since it is difficult to make money from an open-source project, the Typst developers believe that subscribers' fees for the Pro plan will help sustain the project in the longer term. (However, the developers promise that the web app will always have a free tier option.)

The web app is efficiently designed and was inspired by Overleaf's interface (in my estimation). A screenshot of Typst's user interface appears at the beginning of this article; it has a two-pane layout, with your source file (document) in the left pane, and a preview of the compiled document in the right-hand pane.



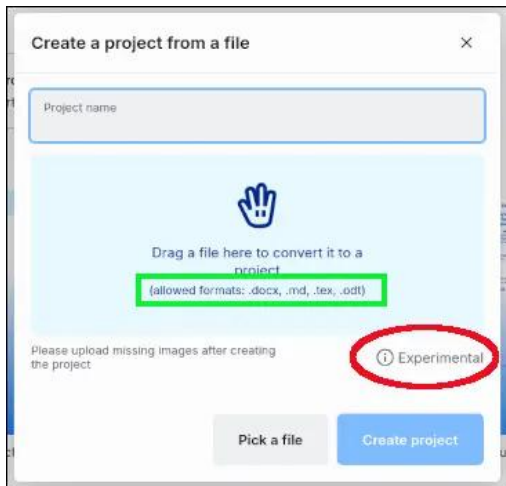
Create a New Document

If you want to create a new document, you can either start from scratch (by clicking on the **Empty document** button) or you can choose an option from the drop-down **Start from template** button (shown below):



Clicking on the **Start from template** option will open a new pop-up window which displays thumbnails of templates from Typst Universe. You can filter the list by category (report, paper, thesis, presentation, CV, etc.) and/or discipline (biology, chemistry, engineering, mathematics, physics, etc.).

One of the options is **Start from a file**; this allows you to import a file and convert it to Typst format (.typ). Supported file formats are: .docx, .md [markdown], .tex and .odt. This feature is labeled as "Experimental" and a pop-up cautions users that "Conversion may not result in the best Typst files, but it is a good starting point."



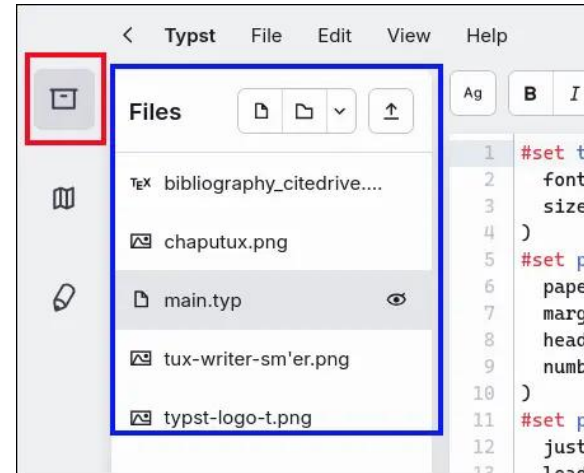
I experimented with importing a LaTeX file (.tex) and a LibreOffice Writer file (.odt). Neither file contained images, and their formatting was straightforward. My .odt file was fine; however, the .tex file was not parsed correctly and a small data chunk was lost. (The source file had an itemized list within a paragraph [accomplished with LaTeX's paralist package]). The Typst converter apparently did not recognize the "inparaenum" environment or know how to process it.)



Toolbar (Left Margin, Upper)

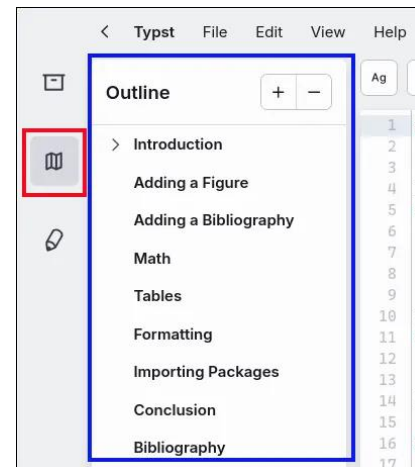
In the upper left margin of the interface, there are three icons.

Explore files [File drawer icon]:



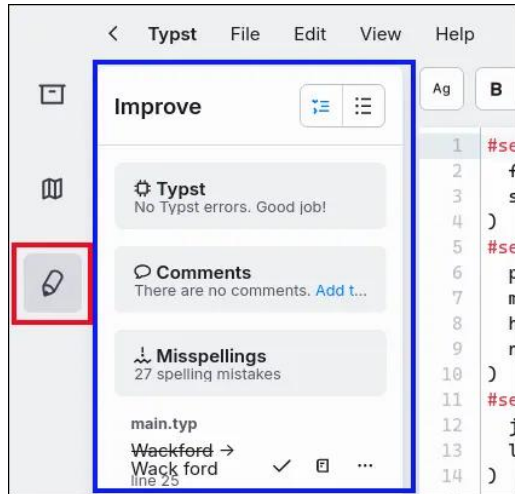
Clicking on this icon opens a new panel in which you can view files associated with your project. In the screenshot above, you can see that in addition to my Typst document (main.typ), I uploaded three image files (.png) as well as a BibTeX bibliography file.

Show outline [Icon of multifold brochure]:



Opens a new panel and displays an outline of your document. The screenshot above shows that my test document has nine sections.

See issues and suggestions [Pencil icon]:



Opens a new panel and displays Typst error messages (with suggestions how to correct the error(s)), reader comments (if you have a paid Typst Pro subscription) as well as misspellings (if you activated the "Enable spellchecking" option in the editor).

Top Toolbar (Upper Left)

On the left side of the toolbar, there is a series of eleven buttons. All buttons have tooltips, so when you hover your cursor over the button, a brief explanation pops up.



The buttons function as follows (proceeding from left to right):

Change Font:

Currently, 119 fonts are available — including various math fonts (such as Fira Math, Lete Sans Math, New Computer Modern Math and the TeX Gyre math fonts [Bonum, Pagella, Schola, Termes]).

Toggle strong/bold text

Toggle emphasized/italic text

Toggle underlined text

Change heading levels:

Changes the heading level from Section to Subsection, then to Subsubsection, etc.

Toggle list:

Creates a bulleted list item (by adding a " - " sign)

Toggle enumeration:

Creates a numbered list item (by adding a " + " sign)

Toggle math mode:

Adds two dollar signs (" \$\$ ") for an inline equation environment.

Toggle code block:

Adds two backticks (" \ ` ") for a 'raw text' environment. This will display the text verbatim and in a monospace font — typically used to embed computer code in your document.

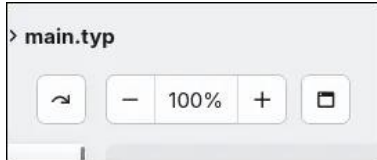
Insert Reference

Add comment:

This feature is only available to paid subscribers with the Typst Pro plan.

Top Toolbar (Middle)

In the middle of the toolbar, you see three buttons:



Scroll preview to cursor position [Curved down arrow icon]:

This will scroll your preview to match the cursor position in the document editor (i.e., the left-hand pane).

Zoom options [Minus sign, 100%, Plus sign]:

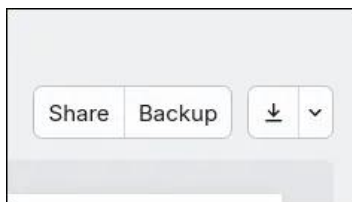
Zoom out or zoom in the displayed preview.

Show preview in popup [Icon of pop-up window with border]:

Displays a preview of your current document in a separate, pop-up window.

Top Toolbar (Right)

In the upper-right corner of the toolbar, there are three buttons:



Share button:

Permits sharing your document with someone else.

Typst allows collaboration via link sharing. Users can create share links (either read-only or read-write) for a document, enabling others — such as a thesis supervisor or co-author — to access the document. However, Typst's free version does not have a built-in comment feature (similar to Overleaf's) which allows collaborators to leave reader comments directly within the document.

I tested this feature by sharing a read-write link with myself (under a different username/e-mail address). It worked fine; after opening the link in an e-mail message, I was taken directly to the shared document and could begin editing its content. No separate login was required.

Backup button:

Downloads a zipped copy (.zip) of your current Typst project.

Quick export PDF [Down arrow icon]:

This button immediately exports your compiled PDF and downloads it to your computer.



Clicking on the right-hand portion of the button triggers a drop-down menu with the options: Export as PDF, PNG (or) SVG

Toolbar (Left Margin, Lower)

Three icons are found in the lower left margin (left):

Open Settings [Gear icon]:

If you are in the Dashboard display, i.e., with no open/active document, you will see settings related to your account, the theme chosen, amount of storage, etc. (Typst's free tier provides 200 MB of storage.)

If a document is open/active, you will see information such as the project name, Typst compiler version, editor font and font size and spellchecker status (on/off).

Typst Universe [Icon of planet Saturn]:

Allows you to explore packages and templates to enhance Typst.

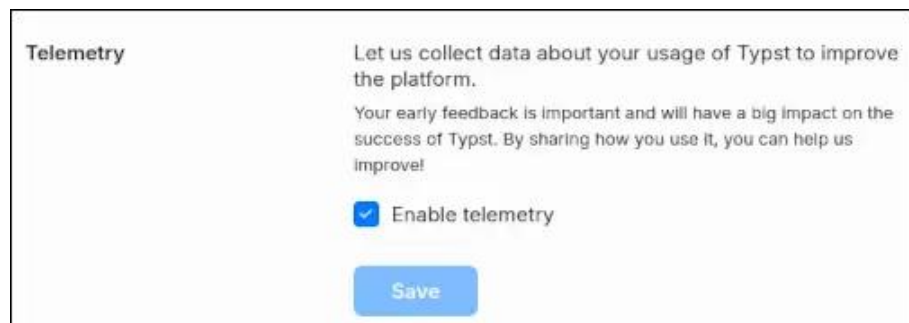
Help [Question mark icon]:

Opens the Typst Documentation website in a new browser tab.

Information Privacy

If you are concerned about information privacy, Typst's policy — in part — states: "Your data is stored in a Microsoft Azure data center in Germany and encrypted at rest ... We can access your documents, but do so only to fix problems on your request or to enforce our terms of service."

You may disable telemetry, if you wish, by clicking on the Gear icon [**Open Settings**] in the lower-left pane of the editor > then look for the section labeled **Telemetry**. Uncheck/untick the **Enable telemetry** box:



Challenges for Typst

For Typst to compete with LaTeX, scientific journals must start accepting submissions in .typ format. That will probably not happen anytime soon

because academia is conservative. (La)TeX has a very well established ecosystem, professors frequently collaborate with it and experienced faculty prefer the tool that they know: LaTeX. For a commercial journal that already accepts LaTeX, there is little incentive to justify the extra cost of accepting Typst submissions as long as there is no large, influential user base demanding it.

Exporting a Typst .typ file to LaTeX format (.tex) is not possible. Martin Haug closed this [issue](#) on GitHub in April 2023 and classified it as "not planned," writing: "We will not directly support LaTeX export as Typst is just too different to provide a satisfactory high-quality conversion. However, the Pandoc project might work on adding a reader for Typst files that will allow medium-fidelity conversion to LaTeX. Alternatively, an approach could be to directly convert the eventual HTML output."

There is a (partial) workaround; user nullst commented that [Pandoc](#) has a working "Typst reader", which means that it can be used to convert Typst code to LaTeX (as well as to HTML, Markdown, and many other formats). However, he noted that conversion is rather lossy, and that moderately complicated documents usually cause parsing errors in Pandoc's reader.

Typst uses its own syntax for math notation. If you are an experienced user who is accustomed to LaTeX's math syntax, switching to Typst's syntax will require some relearning. After browsing a few Reddit discussions on this topic, I conclude that opinions are mixed. Some people believe that Typst's math syntax is cleaner and easier to write; others argue that LaTeX's math syntax is almost universal at this point and/or they spent so much time learning the standard, that they are unwilling to change to anything different.

Users cannot yet draw complex images like with the TikZ package in LaTeX. However, the [CeTZ](#) package in Typst is a library for drawing and plots, which was inspired by TikZ (although not yet as powerful as TikZ). Typst's [Touying](#) package for creating presentation slides is similar to the Beamer class in LaTeX.

Typst currently lacks the ability to export as HTML and ePub, but they are listed as planned features on the development [roadmap](#).

Typst does not support including PDFs as images. (In LaTeX, vector graphics are often inserted as PDF or EPS files.) Neither of those formats are supported as an image format in Typst; the developers acknowledge this as a [limitation](#) because many journals require that figures be submitted in PDF format. They recommend the workaround of converting PDF and EPS images into SVG files with online tools or Inkscape. The Typst web app automatically converts PDF files to SVG files when they are uploaded.

As a brief aside, I would like to dispel the notion that LaTeX development is stagnant. Recent [developments](#) include the LaTeX Tagged PDF project, which extends LaTeX to allow the creation of [accessible PDFs](#) for people with visual impairments. LaTeX2e (the latest stable version) is typically released once a year; if you are interested in reading technical details of the changes, they are explained in a release [newsletter](#).

Is Typst for You?

I cannot answer that question, unfortunately; the answer depends on your workflow and the type of writing you do. Based on my experience, Typst seems well suited to writing scientific articles, math papers, theses, reports and/or technical documentation — the sorts of documents that include equations, tables, figures, bibliographical references, etc.

If you need a typesetting program, are just starting out and only need PDF output, Typst is a good alternative since it is easier to learn than LaTeX. If you are already familiar with LaTeX, that will work to your advantage, and you should be able to learn Typst fairly quickly. Although I do not plan on abandoning LaTeX, I definitely plan to experiment more with Typst. If you are a LaTeX user who relies heavily on specific packages, I suggest that you research beforehand whether Typst supports that functionality.

I am very impressed with Typst and believe it is worth your time — and effort — to explore. I cannot predict Typst's future or potential market share, but its developers have accomplished a tremendous amount in a relatively short time. (We should recall that Donald Knuth originally estimated TeX development would take six months, but ultimately it took nearly ten years!)

I will conclude with the advice that regardless of which typesetting platform you choose, focus on your content first and worry about formatting/layout later.

Additional Resources

Youtuber BamDone [Isaac Weintraub] has produced a series of videos on Typst. The tutorial below is well-structured and informative; it walks you through the process of creating a document in Typst (using the web app). Instead of relying on a template, the presenter demonstrates the syntax / code blocks that you need to accomplish these tasks.

"Getting Started with Typst: Some Basics." [YouTube](#), 5 Apr. 2024. (47 min., 55 sec.)

User sitandr has written an [extended tutorial](#) for Typst; it is a book of educational examples / code snippets. He cautions that the book is unofficial and that although he will try to keep it current, it may contain some outdated information. (Nevertheless, I found his tips helpful.)

For LaTeX users, there is a handy five-page [cheat sheet](#), created by Jianrui Lyu, which lists equivalent Typst function names for LaTeX commands: "Equivalent Typst Function Names of LaTeX Commands."

Typst already has built-in support for the functionality of several popular LaTeX packages. The table below (reproduced from [here](#)) shows frequently loaded packages and their corresponding Typst functions (next page):

If you are interested in seeing a sample of Typst-generated output, I tried to replicate this article using Typst. I have uploaded the PDF [14 p., 1.1 MB] to my [PCLinuxOS Cloud](#) account and shared it from there.

Although the formatting could undoubtedly be improved by someone with more knowledge of Typst, this document shows what you can accomplish even at the introductory level.

LaTeX Package	Typst Alternative
graphicx, svg	image function
tabularx	table , grid functions
fontenc, inputenc, unicode-math	Just start writing!
babel, polyglossia	text function: <code>#set text(lang: "zh")</code>
amsmath	Math mode
amsmath, amssymb	sym module and syntax
geometry, fancyhdr	page function
xcolor	text function: <code>#set text(fill: rgb("#0178A4"))</code>
hyperref	link function
bibtex, biblatex, natbib	cite , bibliography functions
lstlisting, minted	raw function and syntax
parskip	block and par functions
csquotes	Set the text language and type " or '
caption	figure function
enumitem	list , enum , terms functions

Good luck, and enjoy exploring Typst!





 **PCLOS-Talk**
Instant Messaging Server


Sign up TODAY! <http://pclostalk.pclosusers.com>



Help PCLinuxOS Thrive & Survive

DONATE TODAY

 **The PCLinuxOS Magazine**
Created with Scribus

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>

PCLinuxOS

Users Don't
Text
Phone
Web Surf
Facebook
Tweet
Instagram
Video
Take Pictures
Email
Chat
While Driving.

Put Down Your
Phone & Arrive
Alive.



Screenshot Showcase



Posted by francesco_bat, on October 12, 2024, running icewm.



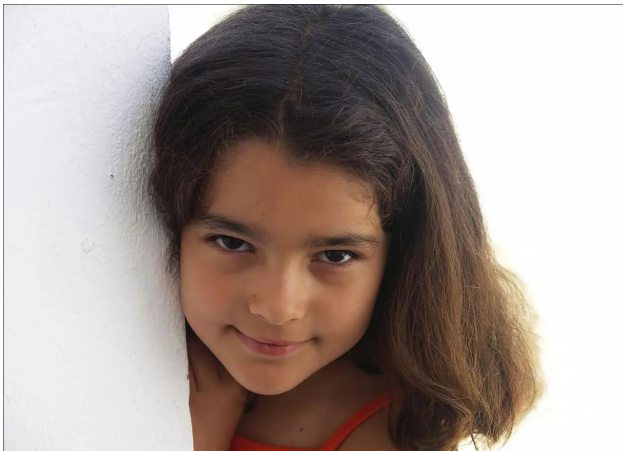
GIMP Tutorial: Create A Double Exposure

by Meemaw

As you know, I look through other sites to find tutorials I think you'll enjoy. I saw this tutorial on [FixThePhoto](#), but when I clicked on the YouTube [video](#), the channel belonged to [Logos by Nick](#). We've seen some of these, and Nick is very skilled.

This is a tutorial for making your photo appear as a double exposure, where there seem to be two distinct photos in the same image. I thought this was fun.

Open your photos in GIMP. I'm going to start with a photo of a little cutie that I got from Wikimedia Commons.



This photo has a background, and we want to get rid of that and just work with the girl. First thing: in the Layers dialog, right-click on the

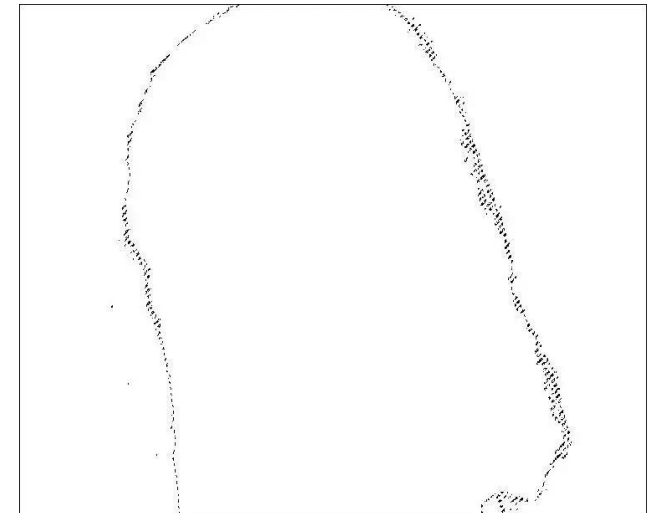
layer with the photo and choose **Add Alpha Channel** (remember, if that menu item is grayed out, the photo already has an alpha channel). Now, you can use your **Fuzzy Select** tool (it looks like a magic wand) to select the background, and press **Delete**. You'll have to do it on each side of the face. On this pic, I selected the whiter background on the left, and had to do it again on the darker. Use it as many times as you need to, in order to remove all the background you want removed.



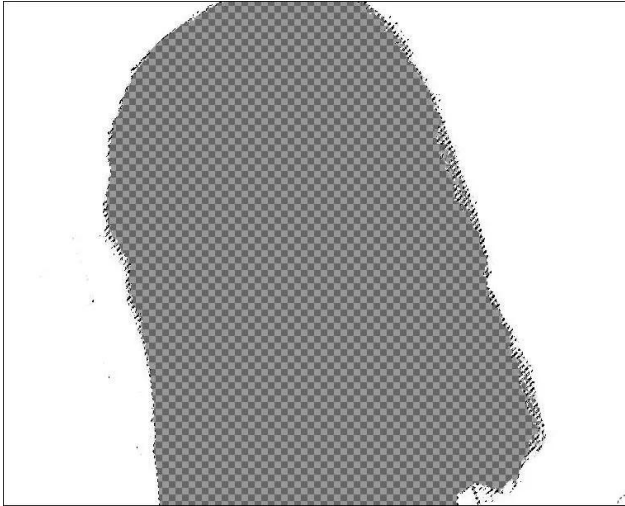
To make our effect work, we need to put another background in, but on another layer. Add a layer, and make the fill white. GIMP will add it above the photo, but we need it under the photo layer. Either click and drag it down, or choose **Lower Layer** in the layers dialog. Also, choose **Select > None** (right, top).



Right-click on the photo layer, and choose **Alpha to Selection**. Now, click the eye to the left on the photo layer, which turns off the visibility of that layer. You should see the following:



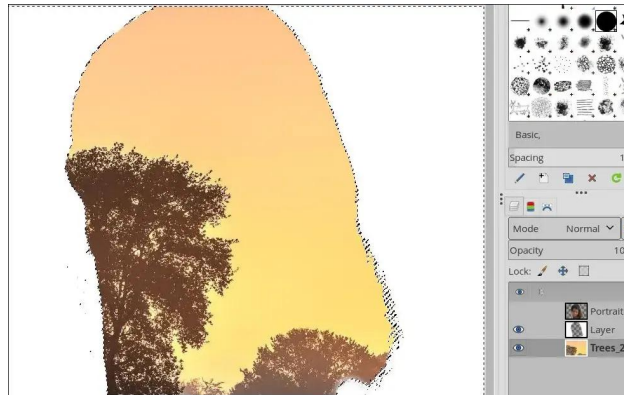
Now, select the white layer, and press the delete key to see this:



Now we'll put in our second photo. I found a sunset with trees that I'm going to use, and will drag it into the same project. Here's the photo:



It needs to be the bottom layer. Here's the photo in place in my project (center, top):

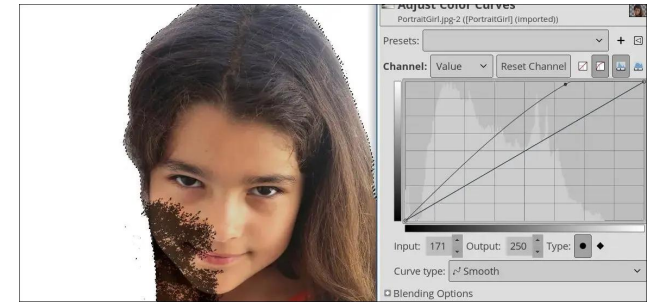


I want it to look kinda like she's seeing around a bush, so I'll mess with it a bit, and move the background layer so it's where I want it. Using the **Move Tool**, you can move your background where you want it. I will re-enable the visibility on my kid photo, and change the layer mode on that photo to **Multiply**.

I may have done something wrong, but I was only able to move the lowest layer with the visibility on the top layer turned off.

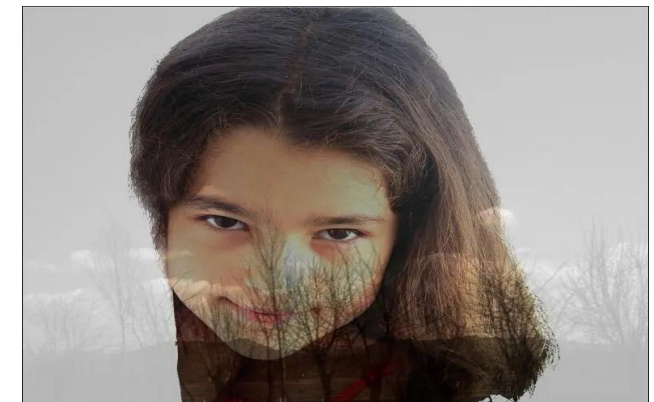
One thing you should do is choose the background and go to **Colors > Desaturate > Desaturate**. It keeps the overall photo from being too dark. The other thing to do is choose the photo layer, go to **Colors > Curves**, and grab the top, right end of the curve and draw it to the left. It keeps the kid's photo from being too dark as well (right, top).

The next thing you can do is choose the white layer, and lower the opacity on it so you can see a hint of the trees through the white (right, center).



When you get it the way you want it, You can export it as whatever image file format you want.

I did several of these. This one had a different background photo.



Tip Top Tips: Backing Up Your /home Directory

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

This month's [tip](#) comes from forum member [davecs](#).

On your PCLinuxOS computer, the folder /home will have a subfolder for every user on the system. If you have a large external drive (and they can be bought cheap these days, though those can be slow), you can back up the /home system onto it easily, using a program called **rsync**. I've also got an extra subfolder in /home, called /home/storage, where I keep stuff safe, like extra fonts, my own wallpaper collection, drivers for my printer/scanner, copies of a few scripts that I like to install when my system needs re-installing, and so on. Of course the main / (root) folder, apart from /home, is installed when I re-install Linux, and if it gets broken somehow, it's probably best to re-install from a more recent iso. Your /home folder stores



Image by [OpenClipart-Vectors](#) from [Pixabay](#)

the personal stuff that you, and everyone else who uses your computer, can't put back from your PCLinuxOS ISO.

What I have done is to format my external drive to ext4, and give it the Volume name "DataBackup". When I plug it to the computer via USB, it gets mounted at /media/DataBackup. I have **rsync** installed, and I have written a little script called "backup", made it executable and put it in /usr/local/bin/, to do the job for me as follows (it needs to be run as root):



```
#!/bin/bash
START=`date +%T`
rsync -aP --exclude-from=/home/storage/
rsync-homedir-excludes/rsync-homedir-
excludes.txt /home/ /media/DataBackup/home
END=`date +%T`
echo Backup started: $START
echo Backup ended: $END
```

Note that from **rsync** to /media/DataBackup/home is all one line.

You get the file rsync-homedir-excludes.txt from this [page](#). In my case, as I use the Vivaldi browser, and Vivaldi uses the same architecture as Google Chrome. I have copied the lines relating to Chrome and changed them for Vivaldi as follows:

#Vivaldi:

```
.config/vivaldi/ShaderCache
.config/vivaldi/*/Local Storage
.config/vivaldi/*/Session Storage
.config/vivaldi/*/Application Cache
.config/vivaldi/*/History Index *
.config/vivaldi/*/Service Worker/
CacheStorage
```

rsync in this case will only write files that either were not on the last backup, or have been updated since the last backup. So the more frequently you run the script, the less time it will take. It will also, during backup, delete files

from the last backup that you have since deleted from your computer. So it's quite a clever program. If you tried to do this either from a file manager using its copy command, or from a terminal using "cp", the outcome would be a total mess.

Finally, I suggest that you also copy the **backup** script to /home/storage so that you will have a copy of it should your computer have an accident wiping your data.



Screenshot Showcase



Posted by DrMop, on October 25, 2024, running Xfce.



*It's easier than $E=mc^2$
It's elemental
It's light years ahead
It's a wise choice
It's Radically Simple
It's ...*

PCLinuxOS
Radically Simple



PCLinuxOS Puzzled Partitions

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

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

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

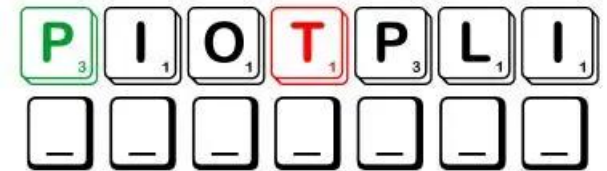
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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

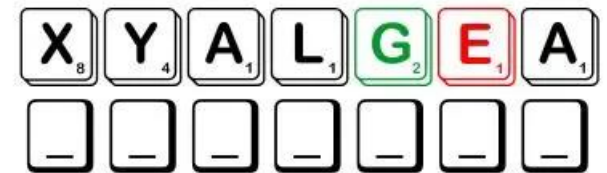


SCRAPPLER RULES:

1. Follow the rules of Scrabble®. You can view them [here](#). You have seven (7) letter tiles with which to make as long of a word as you possibly can. Words are based on the English language. Non-English language words are NOT allowed.
2. Red letters are scored double points. Green letters are scored triple points.
3. Add up the score of all the letters that you used. Unused letters are not scored. For red or green letters, apply the multiplier when tallying up your score. Next, apply any additional scoring multipliers, such as double or triple word score.
4. An additional 50 points is added for using all seven (7) of your tiles in a set to make your word. You will not necessarily be able to use all seven (7) of the letters in your set to form a "legal" word.
5. In case you are having difficulty seeing the point value on the letter tiles, here is a list of how they are scored:
 0 points: 2 blank tiles
 1 point: E, A, I, O, N, R, T, L, S, U
 2 points: D, G
 3 points: B, C, M, P
 4 points: F, H, V, W, Y
 5 points: K
 8 points: J, X
 10 points: Q, Z
6. Optionally, a time limit of 60 minutes should apply to the game, averaging to 12 minutes per letter tile set.
7. Have fun! It's only a game!



Triple Word



Double Word



Download Puzzle Solutions Here

Possible score 247, average score 179.



November 2024 Word Find

Space Exploration

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

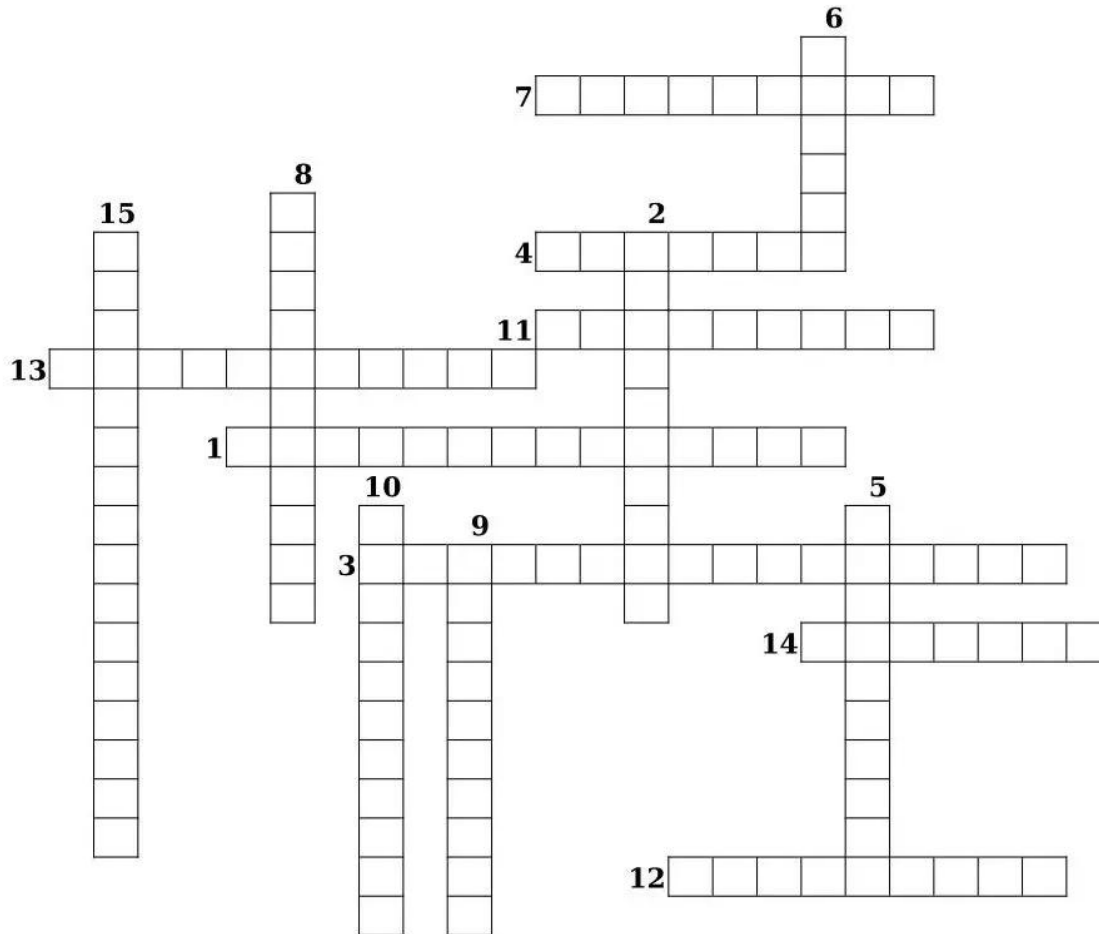
- | | |
|--------------------|------------------|
| AERONAUTICS | ASTRONAUT |
| ASTRONOMER | ATMOSPHERE |
| COMMANDER | COSMOLOGY |
| COSMONAUT | DOCKING |
| ENGINEERS | ENGINES |
| EXTRATERRESTRIAL | FLIGHT |
| GALAXY | GRAVITY |
| HEAT | SHIELDS |
| INTERNATIONAL | INTERSTELLAR |
| LAUNCH | LUNAR MODULE |
| MISSION CONTROL | NAVAL AVIATOR |
| ORBIT | OUTER SPACE |
| PILOT | PLANETS |
| ROCKET | ROCKET SCIENTIST |
| SATELLITE | SCIENTISTS |
| SEA OF TRANQUILITY | SOLAR SYSTEM |
| SPACEWALK | TECHNOLOGY |
| TEST PILOT | |

[Download Puzzle Solutions Here](#)



November 2024 Crossword

Space Exploration



1. The group of people on the ground who direct or control the flight of a spacecraft
2. A person who makes observations of celestial phenomena.
3. A hypothetical or fictional being from outer space, especially an intelligent one.
4. The force that attracts a body toward the center of the earth.
5. The layer of gases that surrounds Earth and contains the air we breathe.
6. A system of billions of stars, together with gas and dust, held together by gravitational attraction.
7. A person who is trained to travel in a spacecraft.
8. An outer covering on a spacecraft, to protect it from the heat generated during re-entry into the earth's atmosphere.
9. The branch of knowledge dealing with engineering or applied sciences.
10. The science or practice of travel through the air.
11. A celestial body orbiting the earth or another planet.
12. A period of physical activity engaged in by an astronaut in space outside a spacecraft.
13. The collection of eight planets and their moons in orbit around the sun, together with smaller bodies in the form of asteroids, meteoroids, and comets.
14. The joining of two separate free-flying space vehicles.
15. A dark spot located in the northern hemisphere of the Moon.

[Download Puzzle Solutions Here](#)

Mixed-Up-Meme Scrambler



Easy for a baker to do.....

HAGUL

--- -- --

ITTYD

--- -- --

SCONED

-- -- --

ARRQUY

-- -- --

" " -----

[Download Puzzle Solutions Here](#)



More Screenshot Showcase



Posted by brisvegas, on October 1, 2024, running Mate.



Posted by bliss, on October 5, 2024, running KDE.



Posted by astronaut, on October 3, 2024, running openbox.



Posted by Archie, on October 1, 2024, running KDE.