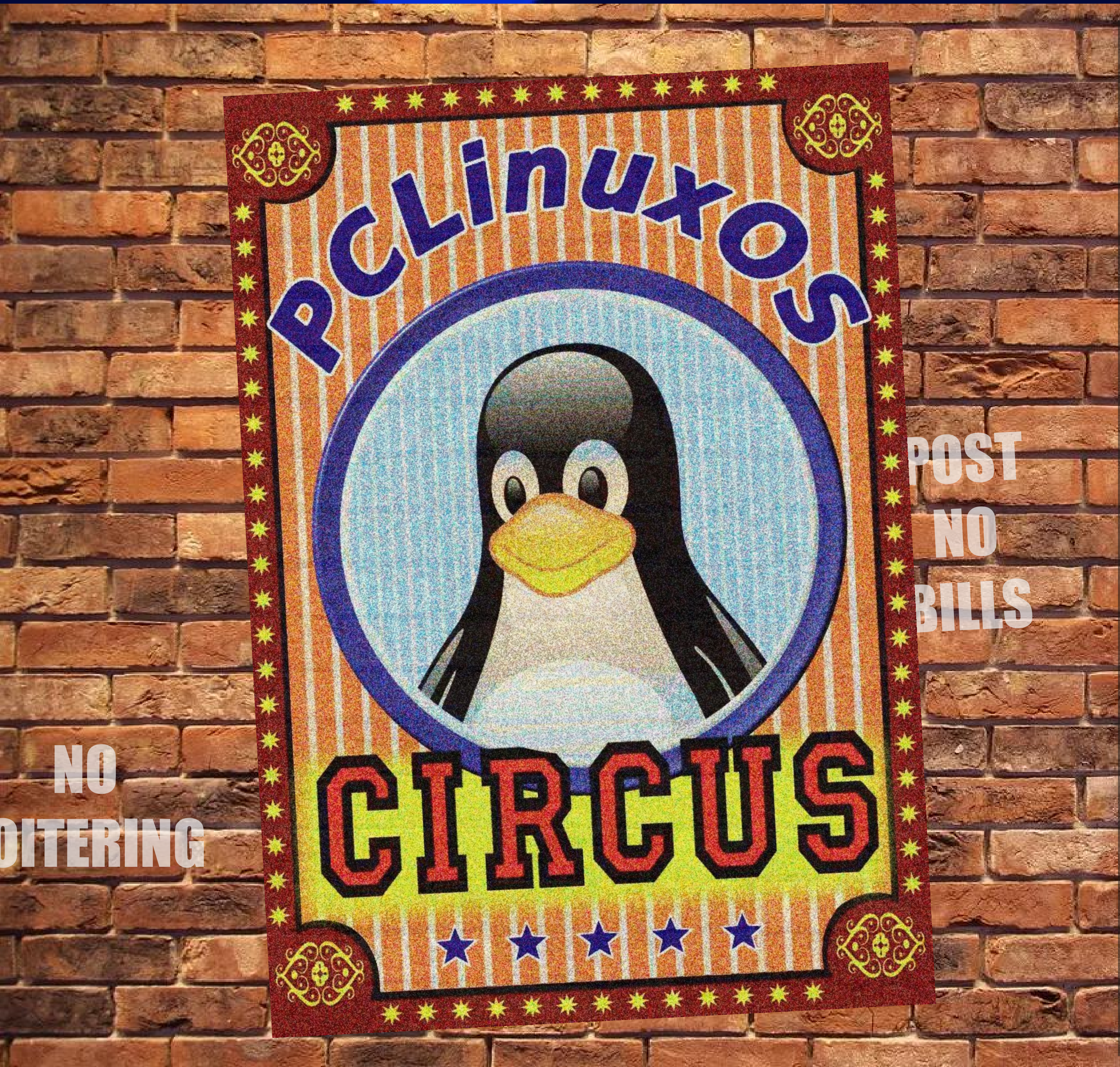
The PCLinuxOS magazine

Volume 222

July, 2025



Inside This Issue...

The PCLinuxOS magazine

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

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

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)

Assistant Editor: Meemaw

Artwork: Paul Arnote, Meemaw

PDF Layout: Paul Arnote, Meemaw

HTML Layout: tbschommer

Staff:

YouCanToo

David Pardue

Alessandro Ebersol

Contributors:

From The Chief Editor's Desk

Undoubtedly, June 2025 is going to go down in the PCLinuxOS history books as the absolute worst month that there ever was. In short, June 2025 was a DISASTER.

No, seriously. Just about everything that could go wrong, did. Maybe we should give it a name, like “The Great June Calamity.”

So, where do I start?

Things certainly started off well enough. From June 13 to June 22, Ryan and I attended Scout camp at H. Roe Bartle Scout reservation in Osceola, MO. Yep. 10 days and nine nights of camping in a canvas tent, sleeping on a canvas cot … and LOTS of walking. Ryan earned his Scout rank, completed most of the requirements for Tenderfoot Scout, and earned three merit badges: Swimming, Leathercraft, and Geology. It was a great (but very tiring) time for us.

But after I got home, things seemed to explode. I started by trying to weed through over 1,000 emails in my inbox. That took me about a day and a half to weed through.

Then, YouCanToo/The CrankyZombie experienced a fire at his house. Now, if you didn’t already know, he hosted PCLinuxOS, the forum, the magazine, PCLOS-Cloud, PCLOS-Talk, pclosmail, the PCLinuxOS Wiki, and ImagStor on servers in his house. His house experienced a significant amount of water and smoke damage. He lost his servers. He lost all of his cameras and lenses. He and his dog were able to get out without injury, but the fire brought almost everything related to PCLinuxOS crumbling down.

I got an email from YCT/TCZ to tell us what had happened. The ONLY thing I could initially find still up and running was the PCLOS Debian forum, so I headed over there. I made an announcement over there about the magazine site, mentioning that all of the other “services” that were being handled by his servers were also down.

Within about a day or so, Texstar set up a temporary forum for PCLinuxOS users. Within the intervening few days, I've witnessed a steady influx of forum regulars showing up in the new, temporary forum. If you haven’t already visited the temporary forum, you should run right over there and sign up for your free account.

In an email update, YCT/TCZ informed me that he wasn’t interested in providing web hosting after this calamity. So, the magazine site is looking for a new web host, and just as soon as we find one (we’re close) and can get the domain transferred, we’ll be back up and running again. Meanwhile, Texstar is looking to possibly move the PCLinuxOS site to another server that he has space on.

We’re still wading through a LOT of unknowns at this point. Like, are the servers totally destroyed? Did the server hard drives survive the fire, smoke, and water damage? Are the backups he made still available? Repairs to YCT/TCZ’s home are expected to take six to eight weeks to complete, so information regarding those questions may not be known for a while yet.

We have been notified that TerryN has backups of the PCLinuxOS Wiki Knowledgebase, and it is currently being hosted here. Just as before (when the Wiki went down during the ransomware attack), only the articles that TerryN has contributed to the wiki are included. As for PCLOS-Cloud, PCLOS-Talk, and pclosmail … well their future is far less certain. Just keep in mind that these services might never return, and if they do, it may take some time before they do (if they do).

Archie Arevalo

2004

January, 2005, holding his newborn daughter

Shortly after establishing the temporary forum, Texstar received word that one of our Global Moderators in the PCLinuxOS Forum, Archie Arevalo, had passed away sometime in May. (Texstar has since re-established a more permanent forum here.)

Archie was a loyal PCLinuxOS user, and loved the KDE desktop. Not hearing from him for extended periods was not unusual, so no one thought that anything was amiss when we hadn’t heard from him for a while.

November, 2016

Born in the Philippines, Archie lived in Changchun, China. There, he met his wife, and they had a daughter in 2005. He was 65 years old. Living behind the “Great Firewall,” it took a while for news of his passing to reach us.

He was also passionate about playing the guitar. Back in 2009, during the “Great Upheaval” in PCLinuxOS’s history, Archie spearheaded a movement to revive The PCLinuxOS Magazine, and tapped me to be its Chief Editor. Archie and I worked closely for a considerable time to put this magazine back on the right path. During that time, he and I became good friends (despite never meeting). Like all friendships, we didn’t always see “eye to eye” sometimes, but we always overcame our differences.

In February, 2024, Archie was in a car accident. He suffered an intracranial hemorrhage, and was hospitalized for about a month. I chatted with him in PCLOS-Talk a couple of months after his accident. He was concerned about his progress … or rather, the lack of progress … in his recovery. He didn't provide a lot of information about the accident or his prognosis, but did provide enough information to "pick my brain" about why he wasn't healing as rapidly as he thought he should (because I worked in a hospital). I assured him that injuries to the body's nervous system were among the slowest to heal.

Knowing Archie, I'm sure he didn't tell me everything … just the things he thought I needed to know to be able to answer his questions. So, there's a real possibility that he purposely didn't reveal the full extent of his injuries. And, having already had an intracranial hemorrhage, there is a heightened risk of another one somewhere down the road.

But the truth of the matter is, we simply don't know what happened to Archie. He tended to keep a lot of his personal details private. All we really know is that he has passed away.

Archie leaves behind his wife and daughter, the latter now enrolled in college.

Unfortunately, with the PCLinuxOS Forum being down, I can't access all the usual information that I normally can when we lose a forum member. Still, Archie's passing deserves attention. He was a kind and compassionate soul, and his influence and insights will be missed in the PCLinuxOS Forum. For Archie, the PCLinuxOS Forum was the house for his second family. His dedication to PCLinuxOS was second to none. R.I.P., our good friend.

****

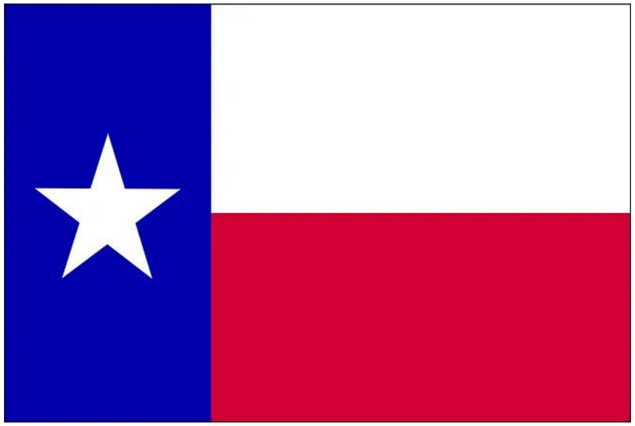
This month's cover is a composite of two separate images from Pixabay. The background image of the brick wall is by Michael Laut. The circus poster image is by José Augusto Camargo, and was modified by Meemaw to customize it for this cover. And, to be completely honest, I didn't know at the time that I designed the cover (early June) how much of a circus things would become with PCLinuxOS.

****

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

ICYMI: N Korean Hackers Use Fake Identities To Land Remote US Tech Jobs

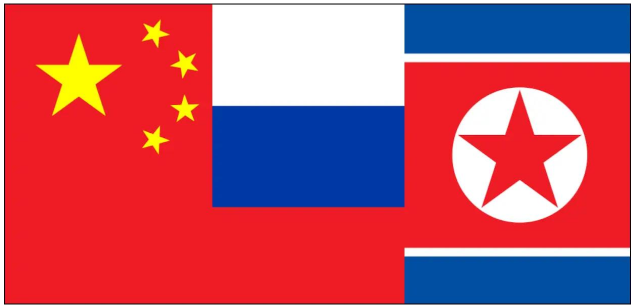
by Paul Arnote (parnote)



A bill requiring Apple and Google to verify the age of users on their app stores is poised to become law in Texas, positioning the state at the center of a growing national debate over regulating smartphone use by children and teens, according to an article from FirstPost. Senate Bill 2420, which passed both chambers of the Texas legislature with a supermajority, now awaits Gov. Greg Abbott's signature. The legislation would require app store operators to verify the age of a device user and, for those under 18, obtain parental consent before allowing app downloads or in-app purchases.

LexisNexis Risk Solutions, a data broker that collects and uses consumers' personal data to help its paying corporate customers detect possible risk and fraud, has disclosed a data breach affecting more than 364,000 people, according to an article from TechCrunch. The company said in a filing with Maine's attorney general that the breach, dating back to December 25, 2024, allowed a hacker to obtain consumers' sensitive personal data from a third-party platform used by the company for software development. Jennifer Richman, a spokesperson for LexisNexis, told TechCrunch that an unknown hacker accessed the company's GitHub account. The stolen data varies, but includes names, dates of birth, phone numbers, postal and email addresses, Social Security numbers, and driver license numbers.

Asus' routers are popular and well-reviewed. As such, there's a good chance you have one of its devices powering your home wifi. If you do, **you should probably check on it, since thousands of Asus' routers are now compromised**, according to an article from Lifehacker. Cybersecurity company GreyNoise published a blog post about this router attack. GreyNoise says attackers used brute-force login attempts (running millions of login attempts until the right match is found) and authentication bypasses (forcing your way in around traditional authentication protocols) to break into these routers. Notably, hackers used authentication bypass techniques that aren't assigned CVEs (common vulnerabilities and exposures). CVEs are labels used to track publicly disclosed security vulnerabilities, which means the security vulnerabilities were either unknown or known only to a limited circle. Once in, hackers exploited the Asus router's CVE-2023-39780 vulnerability to run whatever commands they wanted. Hackers enabled SSH (secure shell) access through Asus' settings, which let them connect to and control the devices. They then stored the configuration—or backdoor—in NVRAM, rather than the disk of the router. The hackers did not leave malware behind, and even disabled logging, which makes their attacks difficult to detect. It's not clear who is behind these attacks.



North Korean hackers operated a "laptop farm" scheme that used fake identities to land remote US tech jobs and illegally collect $17.1 million in wages, according to an article from TechRepublic. The sophisticated scam is part of a broader effort to exploit global labor markets through cybercrime, according to US authorities. Cybersecurity experts described the operation as "something we'd never seen before," citing sophisticated tactics and custom-built programs that enabled the North Koreans to bypass detection systems and exfiltrate sensitive corporate data.

On June 2, Google released out-of-band fixes to address three security issues in its Chrome browser, including one that it said has come under active exploitation in the wild, according to an article from The Hacker News. The high-severity flaw is being tracked as **CVE-2025-5419** (CVSS score: 8.8), and has been flagged as an out-of-bounds read and write vulnerability in the V8 JavaScript and WebAssembly engine. “Out-of-bounds read and write in V8 in Google Chrome prior to 137.0.7151.68 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page,” reads the description of the bug on the NIST's National Vulnerability Database (NVD). Google credited Clement Lecigne and Benoît Sevens of Google Threat Analysis Group (TAG) with discovering and reporting the flaw on May 27, 2025. It also noted that the issue was addressed the next day by pushing out a configuration change to the Stable version of the browser across all platforms. So, if you are a Google Chrome user and you haven’t updated recently, now might be a good time to do so.

Mozilla announced on May 22 that it’s shutting down Pocket, a read-it-later app it acquired in 2017, on July 8, according to an article from TechCrunch. The company is also shutting down Fakespot, its browser extension that helps users identify unreliable reviews. “Pocket has helped millions save articles and discover stories worth reading,” Mozilla said in a blog post. “But the way people use the web has evolved, so we’re channeling our resources into projects that better match their browsing habits and online needs.” Users will be able to continue using the app and browser extensions for Pocket until July 8. After that date, Pocket will move into export-only mode. Users have until October 8 to export saved articles, including items in their list, archive, favorites, notes, and highlights.

Image by Pexels from Pixabay

The latest version of the 'Crocodilus' Android malware has introduced a new mechanism that adds a fake contact to an infected device's contact list to deceive victims when they receive calls from the threat actors, according to an article from BleepingComputer. This feature was introduced along with several others, mostly evasion-focused improvements, as the malware appears to have expanded its targeting scope worldwide. A notable feature in the latest Crocodilus malware version is the ability to add fake contacts on the victim's device. Doing so would cause the device to display the name listed in a caller's contact profile rather than the caller ID when receiving an incoming call. This could allow the threat actors to impersonate trusted banks, companies, or even friends and family members, making the calls appear more trustworthy.

According to an article from Ars Technica, **tracking code that Meta and Russia-based Yandex embed into millions of websites is de-anonymizing visitors by abusing legitimate Internet protocols, causing Chrome and other browsers to surreptitiously send unique identifiers to native apps installed on a device, researchers have discovered**. Google says it's investigating the abuse, which allows Meta and Yandex to convert ephemeral web identifiers into persistent mobile app user identities. The covert tracking — implemented in the Meta Pixel and Yandex Metrica trackers — allows Meta and Yandex to bypass core security and privacy protections provided by both the Android operating system and browsers that run on it. Android sandboxing, for instance, isolates processes to prevent them from interacting with the OS and any other app installed on the device, cutting off access to sensitive data or privileged system resources. Defenses such as state partitioning and storage partitioning, which are built into all major browsers, store site cookies and other data associated with a website in containers that are unique to every top-level website domain to ensure they're off-limits for every other site.

Scammers are targeting travelers planning their vacations in a new campaign that spoofs popular online travel agency (OTA) Booking.com, according to an article from Lifehacker. The scheme, identified by Malwarebytes Labs, uses malicious CAPTCHA forms to gain remote access to victims' devices, allowing threat actors to harvest personal and financial information. The campaign begins with links posted on social media and gaming sites, including sponsored ads, that redirect to websites posing as Booking.com — an OTA through which users can search and book flights, hotels, rental cars, and other travel experiences. When users click the link, they'll see a fake CAPTCHA pop-up with a checkbox, which gives permission to copy data to the clipboard. The next verification prompt will tell you to execute a Run command on your device with a combination of keystrokes. (FYI: This is never a legitimate CAPTCHA request.) In the background, the malicious CAPTCHA has copied a PowerShell command to your clipboard. And if you follow the instructions, the command will download and execute a series of files that install a backdoor Remote Access Tool (RAT)—identified as Backdoor.AsyncRAT—giving threat actors the ability to remotely monitor and control your machine.

Image by Holger Grybsch from Pixabay

The United States has achieved a remarkable breakthrough in hydrogen aviation technology, addressing three critical challenges that previously hindered the development of hydrogen-powered aircraft, according to an article from the Stewartville Star. This innovative system represents a significant step forward in the quest for zero-emission air travel, potentially transforming the aviation industry's environmental impact. Engineers at the FAMU-FSU College of Engineering have developed an integrated system that elegantly solves multiple technical barriers facing hydrogen aircraft. Their creation simultaneously handles hydrogen storage, cooling, and propulsion distribution—all from a single reservoir. This represents a fundamental shift in how aircraft can utilize hydrogen fuel. The system achieves an impressive 0.62 gravimetric index, meaning 62% of the total system mass is dedicated to usable hydrogen. This efficiency significantly outperforms conventional hydrogen storage methods that suffer from excessive auxiliary weight components. Engineers accomplished this through meticulous optimization of vent pressures and heat exchanger dimensions. The aviation sector contributes between 1-2% of global CO emissions according to recent IPCC reports. Hydrogen presents a compelling alternative to traditional jet fuel, offering greater energy density than kerosene while producing zero carbon dioxide emissions during combustion. However, the technical challenges of storing hydrogen at cryogenic temperatures (-253°C) have long prevented practical implementation.

You probably have at least 100 apps on your phone — likely more. And there's plenty of choice, almost 2 million apps on Apple's App Store and nearer 3 million on Google's Play Store. You're urged only to install apps from official stores, but sometimes even that doesn't keep you safe. So it is with **a new list of apps you must delete right now**, according to an article from Forbes. This list comes courtesy of Cyble, whose researchers discovered a raft of apps had tricked their way onto the Play Store despite mimicking the names and icons of legitimate digital wallets. Once installed and opened, the apps open a phishing website or an in-app WebView, requesting the mnemonic phrases that can be used to empty the wallet. Cyble found more than 20 apps, "targeting crypto wallet users" by impersonating "popular wallets such as SushiSwap, PancakeSwap, Hyperliquid, and Raydium," and tricking users into dangerous Play Store installs by using "compromised or repurposed developer accounts." The targeted wallets (and app names) are listed in the article.

OpenAI has revealed that it banned a set of ChatGPT accounts that were likely operated by Russian-speaking threat actors and two Chinese nation-state hacking groups to assist with malware development, social media automation, and research about U.S. satellite communications technologies, among other things, according to an article from The Hacker News. "The [Russian-speaking] actor used our models to assist with developing and refining Windows malware, debugging code across multiple languages, and setting up their command-and-control infrastructure," OpenAI said in its threat intelligence report. "The actor demonstrated knowledge of Windows internals and exhibited some operational security behaviors." The Go-based malware campaign has been codenamed ScopeCreep by the artificial intelligence (AI) company. There is no evidence that the activity was widespread in nature.

Image by William Riccio from Pixabay

June 10, 2025 was **Microsoft's June 2025 Patch Tuesday, which includes security updates for 66 flaws, including one actively exploited vulnerability and another that was publicly disclosed**, according to an article from BleepingComputer. This Patch Tuesday also fixes ten “Critical” vulnerabilities, eight being remote code execution vulnerabilities and two being elevation of privileges bugs. The number of bugs in each vulnerability category is listed as follows: 13 Elevation of Privilege Vulnerabilities, 3 Security Feature Bypass Vulnerabilities, 25 Remote Code Execution Vulnerabilities, 17 Information Disclosure Vulnerabilities, 6 Denial of Service Vulnerabilities, and 2 Spoofing Vulnerabilities. This count does not include Mariner, Microsoft Edge, and Power Automate flaws fixed earlier this month.

Aim Security discovered “EchoLeak”, a vulnerability that exploits design flaws typical of RAG Copilots, allowing attackers to automatically exfiltrate any data from M365 Copilot’s context, without relying on specific user behavior, according to a blog post by Aim Security. The primary chain is composed of three distinct vulnerabilities, but Aim Labs has identified additional vulnerabilities in its research process that may also enable an exploit. You can read Microsoft’s advisory here.

More than 20,000 malicious IP addresses or domains linked to information stealers have been taken down in an INTERPOL-coordinated operation against cybercriminal infrastructure, according to a post from Interpol’s website. During Operation Secure (January – April 2025) law enforcement agencies from 26 countries worked to locate servers, map physical networks and execute targeted takedowns. Ahead of the operation, INTERPOL cooperated with private-sector partners Group-IB, Kaspersky and Trend Micro to produce Cyber Activity Reports, sharing critical intelligence with cyber teams across Asia. These coordinated efforts resulted in the takedown of 79 percent of identified suspicious IP addresses. Participating countries reported the seizure of 41 servers and over 100 GB of data, as well as the arrest of 32 suspects linked to illegal cyber activities.

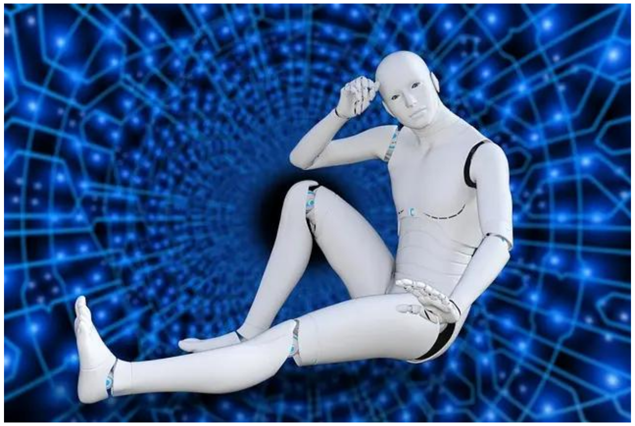
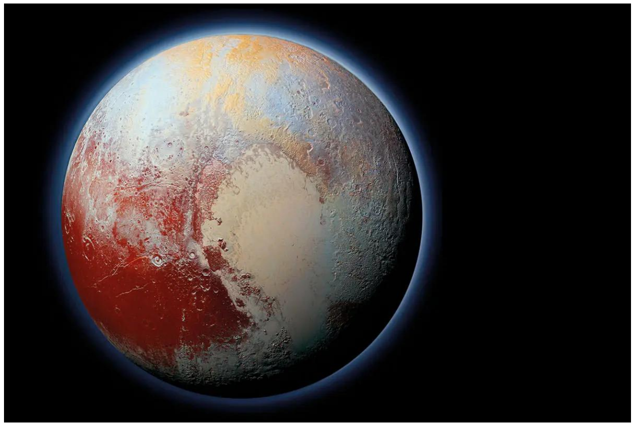


Image by Pete Linforth from Pixabay

A bill that allows artificial intelligence models to be trained on copyrighted material without the rights holders’ knowledge has been passed in the UK, according to an article from TechRepublic. This followed a months-long debate about whether it should be amended to force tech companies to disclose information about their training data. The Data (Use and Access) Bill contains a host of new rules around data sharing, but the most contentious relate to AI. In January, Baroness Beeban Kidron, a House of Lords member, filmmaker, and AI ethics expert, proposed an amendment that would require operators of AI models “to disclose information regarding text and data used in the pre-training, training, and fine-tuning of general-purpose AI models.” She argued that artists and other rights holders deserve transparency and accountability from AI developers, particularly when their work is used without consent to train systems that may later compete with them creatively or commercially. Nevertheless, many members of the House of Commons disagreed. They claimed that the amendment would discourage companies from developing and releasing AI products in the UK, as disclosure requirements would add an undue burden and force them to reveal their proprietary data sources.

We're living in a post-privacy world. Every time you leave the house you're probably on camera. Every time you turn on your television, your viewing habits are being logged. And using the internet in any way is basically just spraying a firehose of your personal information at data brokers — companies that compile your personal information and sell it to marketing companies, people search sites, and anyone else who wants to use it to sell you something, according to an article from Lifehacker. The phrase "data brokers" might conjure up a bunch of shady companies located in countries with loose privacy laws, but some of the biggest are actually familiar companies like Experian, LexisNexis, and Equifax. The data they gather can include your name, address, birthday, phone numbers, income, known associates (like your family members), and everything you do on social media platforms. Anyone with that info can use it to blast you with endless advertisements and spam emails and texts—and if bad actors get a hold of it in a data leak, they can use it maliciously to steal your identity. If you want to beef up your online privacy and help protect yourself from spam and scams, one of the main things you need to do is get your personal data out of the data brokers' servers. You can opt out manually (a tedious, never-ending game of whack-a-mole), or you can pay a service to do it for you.

CAPTCHA — short for "Completely Automated Public Turing test to tell Computers and Humans Apart" — is a form of verification online that helps distinguish human users from bots on login, account sign-up, and e-commerce checkout pages. If you can correctly identify distorted letters or all of the photos that include objects like stop signs to prove you are not a robot, you are permitted to interact with the site or app. But just because CAPTCHA and reCAPTCHA tests are ubiquitous doesn't mean they're always innocuous. Internet users are accustomed to engaging with CAPTCHA without much thought, so naturally, **cybercriminals have found ways to spoof these tests for spreading malware**, according to an article from Lifehacker.



Astronomers using the James Webb Space Telescope (JWST) have taken a fresh look at the distant edges of our solar system — and found that, once again, Pluto is defying expectations, according to an article from LiveScience. When NASA's New Horizons spacecraft flew past Pluto in 2015, it shattered the notion that the dwarf planet was a dormant ball of ice, instead revealing it to be rich with icy plains and jagged mountains. But one of the biggest surprises floated above it all: a bluish, multi-layered haze blanketing the world's sky, stretching more than 185 miles (300 kilometers) above the surface — far higher and more intricate than scientists had predicted. Now, nearly a decade later, new data from JWST confirm that Pluto's haze isn't just a visual oddity, it also controls the dwarf planet's climate.

Instagram ads impersonating financial institutions like Bank of Montreal (BMO) and EQ Bank (Equitable Bank) are being used to target Canadian consumers with phishing scams and investment fraud, according to an article from BleepingComputer. Some ads use AI-powered deepfake videos in an attempt to collect your personal information, while others use official branding to drive traffic outside of the platform to look-alike illicit domains that are not affiliated with banks.

It's a familiar story: your email inbox is bursting with newsletters, sales promos, and spam you don't remember signing up for. **However, attempting to remove it may put your personal information at risk**, according to an article from eSecurity Planet. Cybersecurity experts are now warning that clicking the familiar "unsubscribe" button at the bottom of unwanted emails could lead to phishing scams or malware attacks. According to a DNSFilter report cited by The Wall Street Journal, at least one out of every 644 unsubscribe links leads to a malicious website. This small percentage becomes particularly concerning when multiplied by the billions of spam emails sent daily. Tim Keanini, chief technology officer at DNSFilter, told The Wall Street Journal: “Trust is relative. I trust my email client, but I don’t trust what’s inside the email.” When you click an unsubscribe link, you leave the safe environment of your email app and open a browser, a place where hackers have far more tools to exploit users.

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

Image by Pete Linforth from Pixabay

One-time SMS codes are widely used as the second checkpoint in two-factor authentication (2FA) to sign into everything from banking apps to email accounts. However, SMS is one of the least secure 2FA methods, as it can be phished relatively easily. **It turns out these codes may also be visible to other parties besides the sender (the service generating the code) and the recipient (you), increasing the risk that your accounts can be compromised by bad actors**, according to an article from Lifehacker. As reported by Bloomberg Businessweek, an obscure third-party telecom service had access to at least one million 2FA codes that passed through its network. An investigation led by Bloomberg and Lighthouse Reports — based on data received from an industry whistleblower—found that more than a million text messages containing 2FA codes were visible to Swiss company Fink Telecom Services during June 2023. As an intermediary between the companies that generate authentication codes and the users logging into their accounts, Fink handled the messages and had access to their content. While this is a weakness in SMS—which is unencrypted and relatively easy to intercept—the Fink incident is particularly concerning due to the company's involvement in the surveillance industry and alleged infiltration of user accounts. According to the reporting, the messages came from senders like Google, Meta, Amazon, Tinder, Snapchat, Binance, Signal, WhatsApp, and several European banks and went to recipients in more than 100 countries.

16 billion passwords were exposed in a record-breaking data breach, opening access to Facebook, Google, Apple, and any other service imaginable, according to an article from CyberNews. Unnecessarily compiling sensitive information can be as damaging as actively trying to steal it. For example, the Cybernews research team discovered a plethora of supermassive databases, housing billions upon billions of login credentials. From social media and corporate platforms to VPNs and developer portals, no stone was left unturned. Their team has been closely monitoring the web since the beginning of the year. So far, they’ve discovered 30 exposed datasets containing from tens of millions to over 3.5 billion records each. In total, the researchers uncovered an unimaginable 16 billion records. None of the exposed datasets were reported previously, bar one: in late May, Wired magazine reported a security researcher discovering a “mysterious database” with 184 million records. It barely scratches the top 20 of what the team discovered. Most worryingly, researchers claim new massive datasets emerge every few weeks, signaling how prevalent infostealer malware truly is.

Insurance giant Aflac Incorporated has confirmed it was hit by a cybersecurity breach this month, making it one of the latest casualties in a growing wave of cyberattacks targeting US insurance companies, according to an article from eSecurity Planet. The company says it contained the attack within hours and continues to operate normally, but warns that sensitive customer information may have been exposed. Aflac said it detected “suspicious activity” on its US network on June 12 and quickly activated its cyber incident response protocols. “We promptly initiated our cyber incident response protocols and stopped the intrusion within hours,” the company stated in its official disclosure. Importantly, Aflac noted that “our systems were not affected by ransomware,” and business operations, including underwriting, claims processing, and customer support, remain uninterrupted.

Image by Anja from Pixabay

What are Cats’ meows communicating? AI might have the answer, according to an article from eWEEK. For generations, cat owners have puzzled over what exactly their pets are communicating. Artificial intelligence might be able to help. Scientists and developers are using artificial intelligence to decode feline communication, as reported recently in Scientific American. The AI-driven tools analyze everything from pitch and duration to body movement and even vital signs to detect a cat’s intent. This technology can allegedly decipher whether a cat is hungry, annoyed, affectionate, or something in between.

According to a 23andMe press release, the bankrupt company's holding company reached an agreement with a nonprofit called TTAM for TTAM to buy the company, says an article from Lifehacker. The sale is for "all of the Company’s assets, including the Personal Genome Service (PGS) and Research Services business lines and the Lemonaid Health business, for a purchase price of $305 million." Anne Wojcicki, former CEO of 23andMe, is also at the helm of TTAM. So, in a sense, a company much like the old one is buying its (your) data back. The last-minute bid was supervised by a bankruptcy court, and was deemed to be in keeping with the company's duty to provide the most value to its shareholders. Regeneron told CNN that they did not submit a higher bid “based on our assessment of 23andMe’s remaining value.”

Malwarebytes Labs has identified a tech support scam that uses malicious URLs to embed fake phone numbers within legitimate site searches, according to an article from Lifehacker. This scam begins, as many do, with a sponsored ad on Google. If you search for a company's tech support phone number, you may see several (fake) results near the top of the page. Often, clicking these links will take you to a fake phishing website that you can identify by checking the URL, but in some cases, you'll actually land on the legitimate support page with little cause for suspicion. However, the number displayed may be fraudulent, and if you call, you'll reach scammers rather than tech support. This type of attack allows cybercriminals to embed phone numbers within an authentic site, where they are prominently displayed. Once on the phone, scammers will request login credentials, financial account information, or even remote access to your device. Because the URL is legitimate and the page layout authentic, you may not think twice about calling the number. Malwarebytes has found this attack on sites that include Netflix, PayPal, Apple, Microsoft, Facebook, Bank of America, and HP.

Image by Markus Spiske from Pixabay

Distributed-denial-of-service (DDoS) attacks usually use a network of compromised devices to bombard a server with an unusually large amount of data in order to render a service unusable. **But Cloudflare says it recently blocked a monumental DDoS attack which attempted to dump almost 38TB worth of data in just 45 seconds — making it the largest such attack in history**, according to an article from TechRadar. For comparison, 38TB is the equivalent of downloading 9,350 full-length HD movies, or 9.35 million songs, or 7,480 hours of high-definition video.

A new version of the Android malware "Godfather" creates isolated virtual environments on mobile devices to steal account data and transactions from legitimate banking apps, according to an article from Bleeping Computer. These malicious apps are executed inside a controlled virtual environment on the device, enabling real-time spying, credential theft, and transaction manipulation while maintaining perfect visual deception. The tactic resembles that seen in the FjordPhantom Android malware in late 2023, which also used virtualization to execute SEA bank apps inside containers to evade detection. However, Godfather's targeting scope is much broader, targeting over 500 banking, cryptocurrency, and e-commerce apps worldwide using a full virtual filesystem, virtual Process ID, intent spoofing, and StubActivity.

Astronomers have revealed a nearby spiral galaxy in all its brilliant glory, shining in thousands of colors, according to an article that appeared on Audacy, from the Associated Press. The dazzling panoramic shot released Wednesday of the Sculptor galaxy by a telescope in Chile is so detailed that it's already serving as a star-packed map. Scientists used the European Southern Observatory's Very Large Telescope to observe the galaxy for some 50 hours, stitching together more than 100 exposures to create the picture. The image spans 65,000 light-years, almost the entire galaxy. A light-year is 5.8 trillion miles. Sculptor — officially labeled NGC 253 — is considered a starburst galaxy, one heavy with stellar action. It's located 11 million light-years away in the Southern Hemisphere's constellation Sculptor, and easy to view with binoculars or small telescopes.

Image by Bernd from Pixabay

Your phone buzzing nonstop? You're not alone, according to an article from Cord Cutters News. Americans are drowning in a deluge of robocalls, with nearly 5 billion hitting phones last month alone, according to YouMail, a call screening and blocking service. That's an eye-watering average of over 1,803 robocalls per second in May, marking an 11% spike in the first five months of 2025 compared to the same period in 2024. The data paints a grim picture for those hoping for a quieter phone line, with smaller and mid-sized cities bearing the brunt of this relentless wave.

Google has introduced Gemini CLI, a free, open-source AI tool designed to work directly in the developer's terminal, according to an article from TechRepublic. The company says it wants to bring the power of Gemini into the hands of coders in the most native way possible: through the command line. The Gemini CLI is powered by the Gemini 2.5 Pro model, which features an impressive 1 million-token context window, allowing for the easy analysis of large codebases or documents. It's all built under the Apache 2.0 license, meaning developers can freely inspect, modify, or extend the software. The tool can read files, execute commands, edit scripts, and even invoke Google Search results in real time to assist with context-sensitive tasks. For those who prefer hands-on control, the agent is extensible via the Model Context Protocol (MCP) and can integrate with external tools and data sources.

Microsoft's iconic Blue Screen of Death (BSOD) is dead after 40 years. RIP to the most panic-inducing screen a Windows user can encounter, according to an article from Lifehacker. Now, get ready to fear the Black Screen of Death. In a blog post on its website today, the company revealed it's ready to go live with an error screen redesign it's been testing since March. In an update to all Windows 11, version 24H2 devices coming "later this summer," the BSOD will finally be put out of its misery. It's likely to be a bittersweet moment for Windows users, who will undoubtedly have mixed feelings about the warning's fate. Despite its ominous name, getting a BSOD wasn't always as serious as it seemed—a simple crash could trigger it, and restarting could easily fix it. It could be worse than that, too, but in many cases, the old BSOD simply added a bit of personality to the most annoying interruptions to your workflow. Especially in recent years, when you would see a sideways frowning emoticon alongside your error message. By the way, did you notice that the ONLY thing that changed is the color of the screen? The acronym remains the same: BSOD.

Disclaimer

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

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

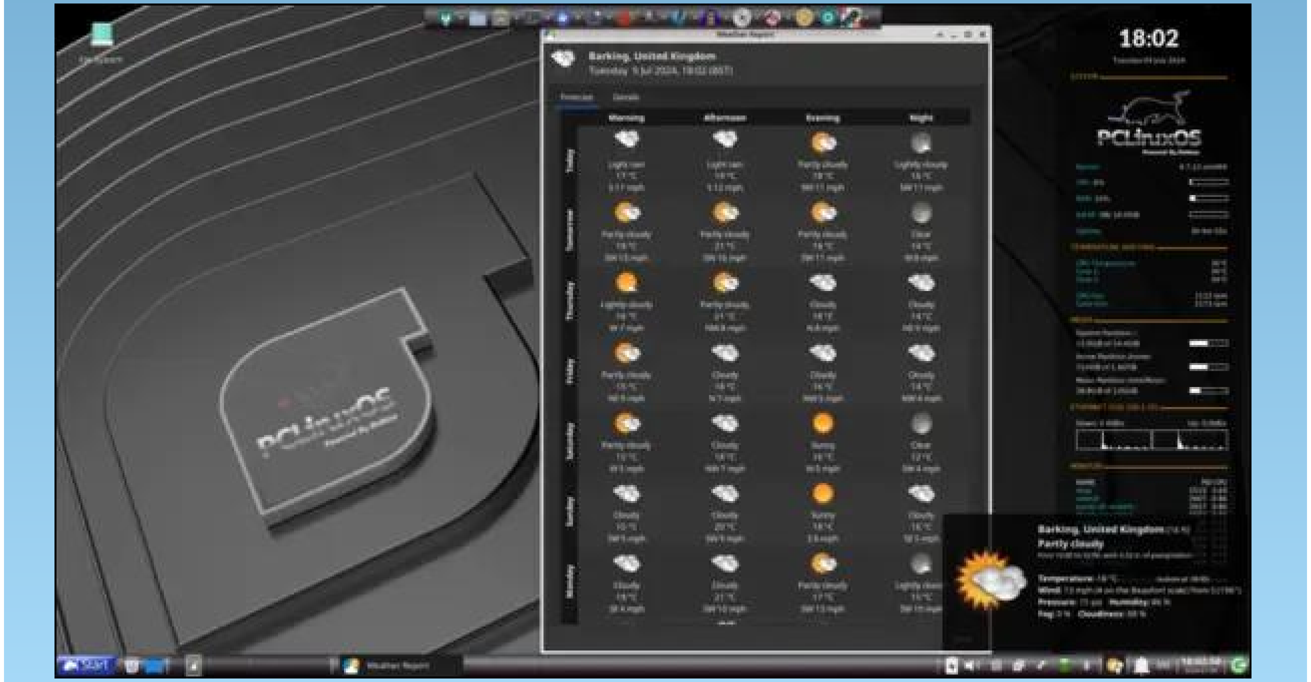
3. The PCLinuxOS Magazine and its associates shall not be liable, at any time, for damages (including, but not limited to, without limitation, damages of any kind) arising in contract, rot or otherwise, from the use of or inability to use the magazine, or any of its contents, or from any action taken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

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

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

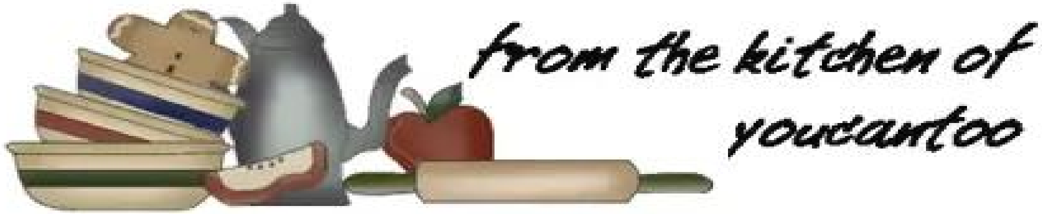
Entire Agreement: These terms constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.

Screenshot Showcase



Posted by davecs, on July 9, 2024, running PCLOSDebian Xfce.

PCLinuxOS Recipe Corner



Quick Garlic Butter Steak Noodle

Serves: 4

INGREDIENTS:

For the Steak:
1 lb steak (sirloin or ribeye), thinly sliced
1 tablespoon cornstarch
½ teaspoon salt
½ teaspoon black pepper
1 tablespoon vegetable oil

For the Noodles:
8 oz ramen or lo mein noodles
2 tablespoons butter
4 cloves garlic, minced
¼ teaspoon red pepper flakes (optional)
¼ cup soy sauce
1 tablespoon oyster sauce
1 tablespoon honey
1 teaspoon sesame oil
½ cup beef broth

For Garnish:
2 green onions, sliced
1 teaspoon sesame seeds

DIRECTIONS:

Cook the Noodles: Boil noodles according to package instructions. Drain and set aside.
Prepare the Steak: Toss sliced steak with cornstarch, salt, and black pepper.
Cook the Steak: Heat vegetable oil in a skillet over high heat. Sear steak for 2–3 minutes until browned. Remove and set aside.
Make the Sauce: In the same skillet, melt butter and sauté garlic for 30 seconds. Add red pepper flakes, soy sauce, oyster sauce, honey, sesame oil, and beef broth. Simmer for 1–2 minutes.
Combine Everything: Return steak to the skillet, add noodles, and toss until fully coated in the sauce.
Serve: Garnish with green onions and sesame seeds.

NUTRITION:

Calories: 580 Carbs: 40g Sodium: 750mg
Fiber: 2g Protein 30g

Two Courts Rule On Generative AI & Fair Use — One Gets It Right

by **Tori Noble**
Electronic Frontier Foundation

Things are speeding up in generative AI legal cases, with two judicial opinions just out on an issue that will shape the future of generative AI: whether training gen-AI models on copyrighted works is fair use. One gets it spot on; the other, not so much, but fortunately in a way that future courts can and should discount.

The core question in both cases was whether using copyrighted works to train Large Language Models (LLMs) used in AI chatbots is a lawful fair use. Under the US Copyright Act, answering that question requires courts to consider:

1. whether the use was transformative;

2. the nature of the works (Are they more creative than factual? Long since published?)

3. how much of the original was used; and

4. the harm to the market for the original work.

In both cases, the judges focused on factors (1) and (4).

The right approach

In *Bartz v. Anthropic*, three authors sued Anthropic for using their books to train its Claude chatbot. In his order deciding parts of the case, Judge William Alsup confirmed what EFF has said for years: fair use protects the use of copyrighted works for training because, among other things, training gen-AI is "transformative—spectacularly so" and any alleged harm to the market for the original is pure speculation. Just as copying books or images to create search engines is fair, the court held, copying books to create a new, "transformative" LLM and related technologies is also protected:

> *[U]sing copyrighted works to train LLMs to generate new text was quintessentially transformative. Like any reader aspiring to be a writer, Anthropic's LLMs trained upon works not to race ahead and replicate or supplant them—but to turn a hard corner and create something different. If this training process reasonably required making copies within the LLM or otherwise, those copies were engaged in a transformative use.*

Importantly, Bartz rejected the copyright holders' attempts to claim that any model capable of generating new written material that might compete with existing works by emulating their "sweeping themes, "substantive points," or "grammar, composition, and style" was an infringement machine. As the court rightly recognized, building gen-AI models that create new works is beyond “anything that any copyright owner rightly could expect to control.”

There’s a lot more to like about the *Bartz* ruling, but just as we were digesting it, *Kadrey v. Meta Platforms* came out. Sadly, this decision bungles the fair use analysis.

A fumble on fair use

Kadrey is another suit by authors against the developer of an AI model, in this case Meta’s ‘Llama’ chatbot. The authors in Kadrey asked the court to rule that fair use did not apply.

Much of the *Kadrey* ruling by Judge Vince Chhabria is dicta — meaning, the opinion spends many paragraphs on what it thinks could justify ruling in favor of the author plaintiffs, if only they had managed to present different facts (rather than pure speculation). The court then rules in Meta’s favor because the plaintiffs only offered speculation.

But it makes a number of errors along the way to the right outcome. At the top, the ruling broadly proclaims that training AI without buying a license to use each and every piece of copyrighted training material will be “illegal” in “most cases.” The court asserted that fair use usually won’t apply to AI training uses even though training is a “highly transformative” process, because of hypothetical “market dilution” scenarios where competition from AI-generated works could reduce the value of the books used to train the AI model.

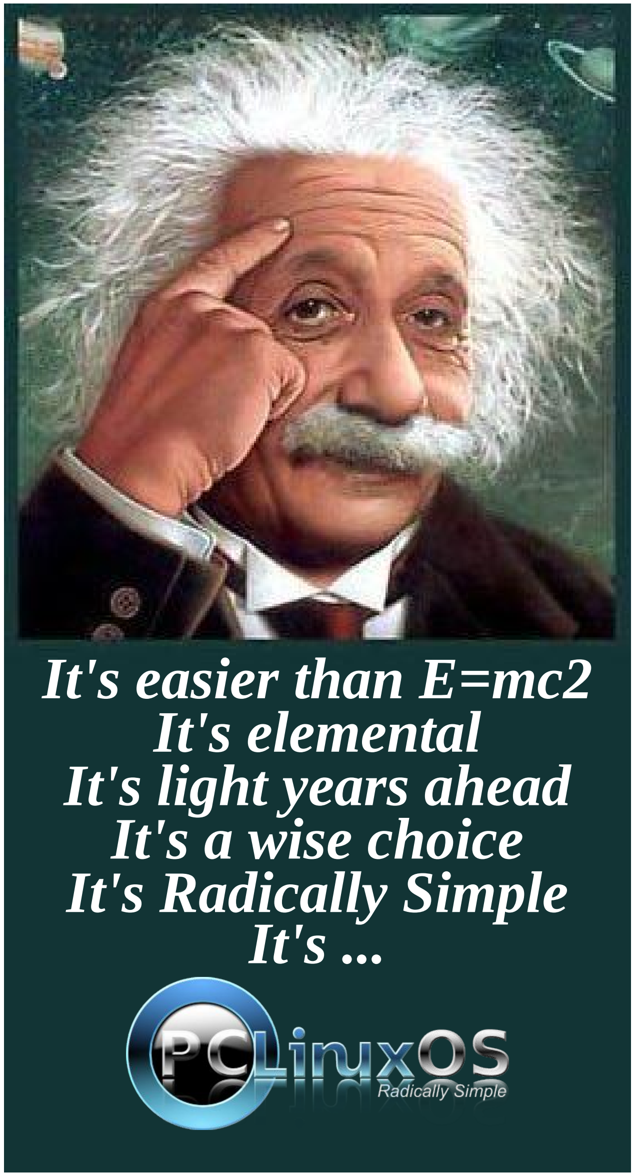
That theory, in turn, depends on three mistaken premises. First, that the most important factor for determining fair use is whether the use might cause market harm. That’s not correct. Since its seminal 1994 opinion in *Cambell v Acuff-Rose*, the Supreme Court has been very clear that no single factor controls the fair use analysis.

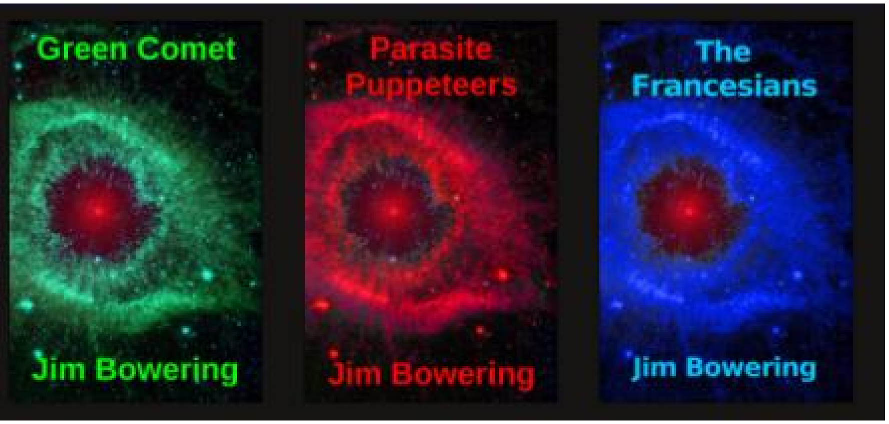
Second, that an AI developer would typically seek to train a model entirely on a certain type of work, and then use that model to generate new works in the exact same genre, which would then compete with the works on which it was trained, such that the market for the original works is harmed. As the *Kadrey* ruling notes, there was no evidence that Llama was intended to do, or does, anything like that, nor will most LLMs for the exact reasons discussed in Bartz.

Third, as a matter of law, copyright doesn't prevent “market dilution” unless the new works are otherwise infringing. In fact, the whole purpose of copyright is to be an engine for new expression. If that new expression competes with existing works, that’s a feature, not a bug.

Gen-AI is spurring the kind of tech panics we’ve seen before; then, as now, thoughtful fair use opinions helped ensure that copyright law served innovation and creativity. Gen-AI does raise a host of other serious concerns about fair labor practices and misinformation, but copyright wasn’t designed to address those problems. Trying to force copyright law to play those roles only hurts important and legal uses of this technology.

In keeping with that tradition, courts deciding fair use in other AI copyright cases should look to *Bartz*, not *Kadrey*.





Screenshot Showcase

Posted by luikki, on July 2, 2025, running KDE.

Typst Cookbook, Part Three

by David Pardue (kalwisti)

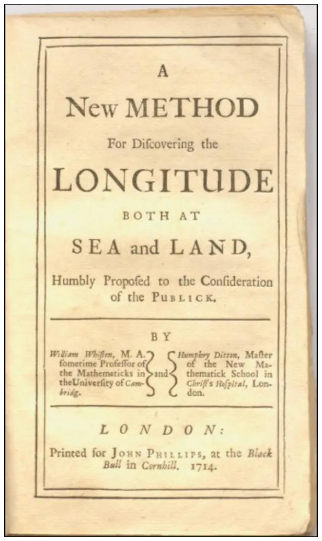
I will conclude this Cookbook series by focusing on how to create a title page for your Typst project. Although not every document needs a separate title page, formatting one can involve a fair amount of trial and error. I hope these “recipes” will save you time and effort.

Brief History of the Title Page

The first printed books, or incunabula (from the Latin word incunabulum ['cradle' or 'swaddling clothes', hence 'beginning']), did not have title pages. The text simply begins on the first page, and the book is often identified by the initial words—the incipit (from the verb incipere ['to begin'])—of the text proper. Other older books may have bibliographic information in the colophon (derived from the Greek word κολοφών ['summit' or 'finishing touch']) at the end of the book.

Early printers produced the pages of a text: the text block. The text block was sold unbound, as a stack of pages. Since print shops were physically demanding, messy environments, the first page of a text block often became scuffed. Printers began making cover pages with some basic identifying information, for convenience and protection of the actual pages. This cover page gradually evolved into a full title page with publication details as well as the author and title.

A title page typically includes the document title, author name(s), institutional affiliation, publication date and other relevant information (such as a translator's name, illustrator, edition statement). The appearance of title pages has changed according to period fashions, e.g., the elaborate title pages of the 17th – 19th centuries, with their extensive subtitles and detailed author/publisher information (often set in multiple typefaces within decorative frames):



A

New METHOD

For Diſcovering the

LONGITUDE

BOTH AT

SEA and LAND,

Humbly Propoſed to the Conſideration
of the PUBLICK.

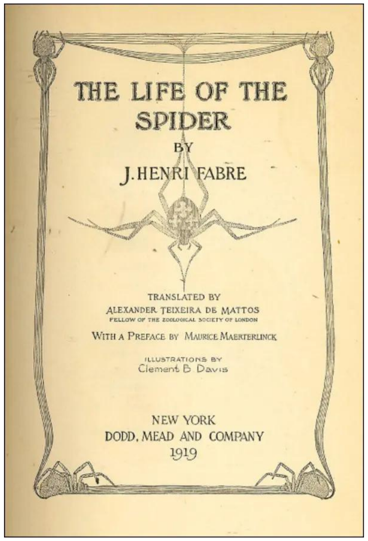
BY

William Whiſton, M. A. ſometime Profeſſor of the Mathematicks in the Univerſity of *Cambridg*. and *Humphry Ditton*, Maſter of the New Mathematick School in *Chriſt's Hoſpital*, London.

LONDON:

Printed for JOHN PHILLIPS, at the *Black Bull* in *Cornhill*. 1714.

Below is the title page of a monograph by French entomologist Jean-Henri Fabre (1823–1915). In addition to the typical information, it lists the translator, the author of the preface and the illustrator. The realistic spider illustrations also convey a sense of the book's style: a non-fiction work intended for adults.



THE LIFE OF THE
SPIDER

BY

J. HENRI FABRE

TRANSLATED BY
ALEXANDER TEIXEIRA DE MATTOS
FELLOW OF THE ZOOLOGICAL SOCIETY OF LONDON

WITH A PREFACE BY MAURICE MAERTERLINCK

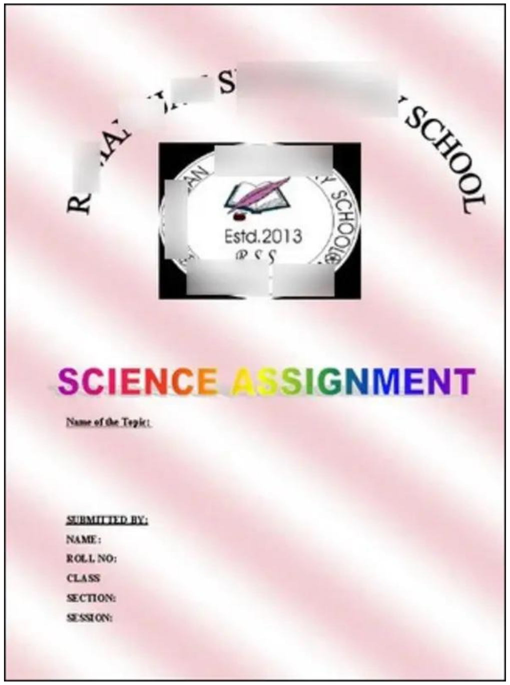
ILLUSTRATIONS BY
Clement B Davis

NEW YORK
DODD, MEAD AND COMPANY
1919

Design Considerations

The title page sets the tone for your document and makes a first impression on your reader. Besides providing essential bibliographic information, it establishes credibility and guides the reader into your document. Readers typically form judgments about document quality within 7–10 seconds of viewing the title page.

A cardinal rule is to avoid inappropriate font choices that do not match your document's tone. For instance, using decorative fonts—such as Comic Sans—in academic papers or overly formal typography in creative projects undermines your document's purpose. Your readers may take you less seriously if your title page showcases Microsoft Word's Rainbow Text and WordArt effects.



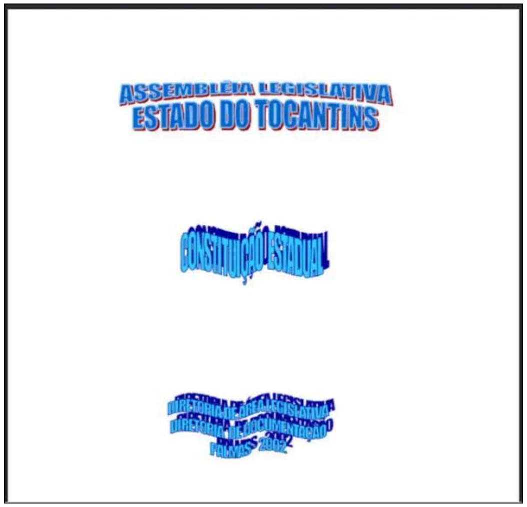
SCHOOL

Estd.2013

SCIENCE ASSIGNMENT

Name of the Topic:

SUBMITTED BY:
NAME:
ROLL NO:
CLASS
SECTION:
SESSION:



ASSEMBLÉIA LEGISLATIVA
ESTADO DO TOCANTINS

CONSTITUIÇÃO ESTADUAL

DIRETORIA DE ÁREA LEGISLATIVA
DIRETORIA DE DOCUMENTAÇÃO
PALMAS 2002

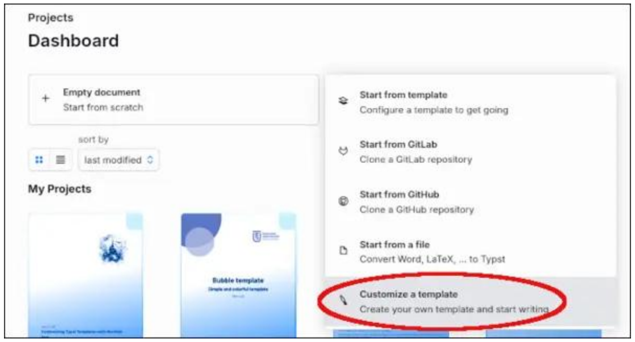
(Fun fact: The 2002 edition of the constitution of the Brazilian state of Tocantins has a title page created with WordArt [image at right]. The 2024 edition has a more contemporary layout, thankfully.)

Avoid overcrowding your title page with unnecessary information; white space is as effective in a layout as type. Avoid excessive artwork or embellishments—complex fonts or too many fonts. A clean, simple layout is preferable. Another point to remember is that typography is a craft, not a science; it can be tricky to discern what is appropriate and what is not.

Disclaimer: I have a long-standing interest in typography, but I am not a book designer. I worked as a cataloging librarian for thirty years, so I have seen my fair share of title pages, half-title pages, frontispieces, title page versos and book covers. (For printed books, the title page is the “chief source of information” or the “preferred source” of bibliographic data which catalogers use to prepare a bibliographic description.) The examples below are not professional grade, but I believe they will give you reasonable templates upon which to build.

Customizing Templates via Typst's Web App

The simplest way to create a serviceable title page is to use the “**Customize a template**” option in Typst's web app. It features a wizard with a checklist of various elements in your document and allows you to configure how they will be laid out.



Projects
Dashboard

Empty document
Start from scratch

sort by: last modified

My Projects

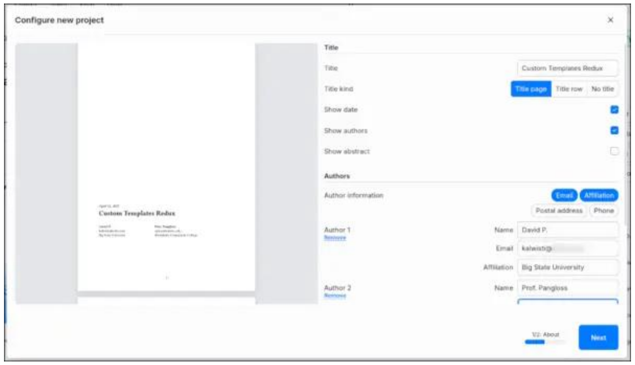
Start from template
Configure a template to get going

Start from GitLab
Clone a GitLab repository

Start from GitHub
Clone a GitHub repository

Start from a file
Convert Word, LaTeX, ... to Typst

Customize a template
Create your own template and start writing



Configure new project

Title

Title: Custom Templates Redux
Title kind: [✓ Title page] Title row No title
Show date ☑
Show authors ☑
Show abstract □

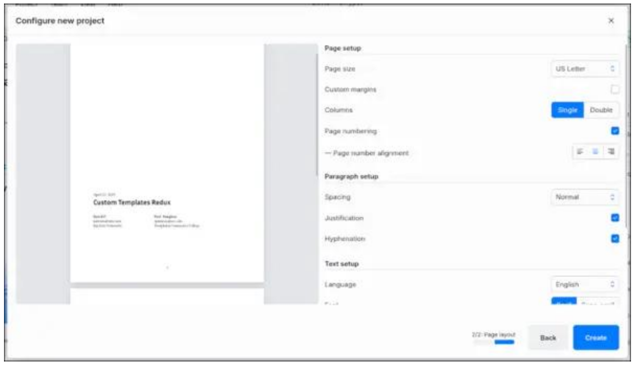
Authors

Author information: [✓ Email] [✓ Affiliation] Postal address Phone

Author 1 (Remove)
Name: David P.
Email: kalwisti@
Affiliation: Big State University

Author 2 (Remove)
Name: Prof. Pangloss

1/2: About
Next



Configure new project

Page setup

Page size: US Letter
Custom margins □
Columns: [✓ Single] Double
Page numbering ☑
— Page number alignment

Paragraph setup

Spacing: Normal
Justification ☑
Hyphenation ☑

Text setup

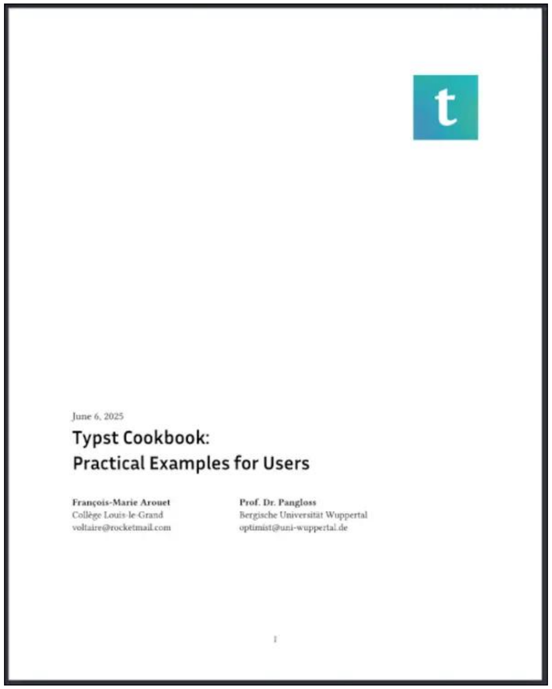
Language: English

2/2: Page layout
Back
Create

I created a Typst project using the wizard and selected several options related to my title page layout, such as (next page):

- **Title kind**: *Title page*
- **Show date**: (checked/ticked)
- **Show authors**: (checked/ticked)
- **Author information** [in a grid]: *Author 1*,
  Author 2
  - · (Also display): *Email*, *Affiliation*
- **Page numbering**: (checked/ticked)
- **Page number alignment**: (centered)

(I did not list every configuration option in order to save space.) The resulting title page (below) is clean and attractive:



June 6, 2025

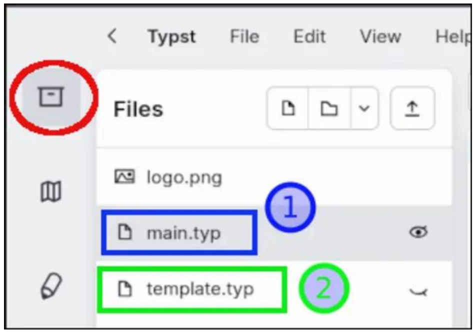
Typst Cookbook:
Practical Examples for Users

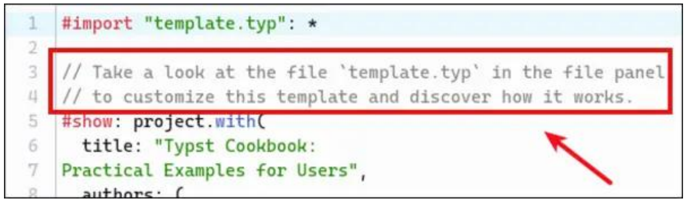
François-Marie Arouet
Collège Louis-le-Grand
voltaire@rocketmail.com

Prof. Dr. Pangloss
Bergische Universität Wuppertal
optimist@uni-wuppertal.de

1

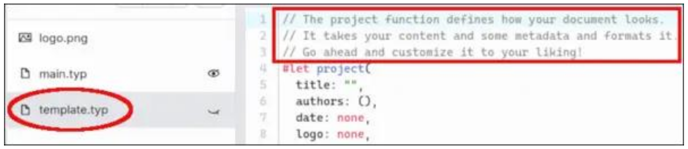
A nice feature of this tool is that your project will contain two files in the file manager (“**Explore files**”): *main.typ* and *template.typ*. Each file is commented with instructions to help you further customize your document (center, top).





```
#import "template.typ": *

// Take a look at the file `template.typ` in the file panel
// to customize this template and discover how it works.
#show: project.with(
  title: "Typst Cookbook:
Practical Examples for Users",
  authors: (
```



```
// The project function defines how your document looks.
// It takes your content and some metadata and formats it.
// Go ahead and customize it to your liking!
#let project(
  title: "",
  authors: (),
  date: none,
  logo: none,
```

To achieve my title page result shown in the screenshot, I only had to make two modifications to the files. To add the Typst logo (the stylized “t”) in the upper right corner, I first downloaded its .png file from Typst's GitHub page, then renamed it as “*logo.png*” and uploaded the file to my project.

In the main.typ file, I added a line with the argument logo: “*logo.png*” (as indicated in the code below):

```
#show: project.with(
     title: "Typst Cookbook:
Practical Examples for Users",
     authors: (
        (name: "François-Marie Arouet",
affiliation: "Collège Louis-le-Grand",
email: "voltaire@rocketmail.com"),
          (name: "Prof. Dr. Pangloss",
affiliation: "Bergische Universität
Wuppertal", email: "optimist@uni-
wuppertal.de"),
     ),
     logo: "logo.png",
     date: "June 6, 2025",
)
```

The width of the logo can be adjusted by the image's width parameter in the template.typ file—16% in this case:

```
// Title page.
     // The page can contain a logo if
you pass one with `logo: "logo.png"`.
     v(0.6fr)
     if logo != none {
          align(right, image("logo.png",
width: 16%))
}
```

I also decided to modify the arrangement of the Author Information by shifting the E-mail address to the line below the Author Affiliation. This was easily done by changing the order listed in the template.typ file:

```
// Author information.
pad(
     top: 0.7em,
     right: 20%,
     grid(
          columns: (1fr,) * calc.min(3,
authors.len()),
          gutter: 1em,
          ..authors.map(author =>
align(start)[
          *#author.name* \
          #author.affiliation \
          #author.email \
        ]),
    ),
)
```

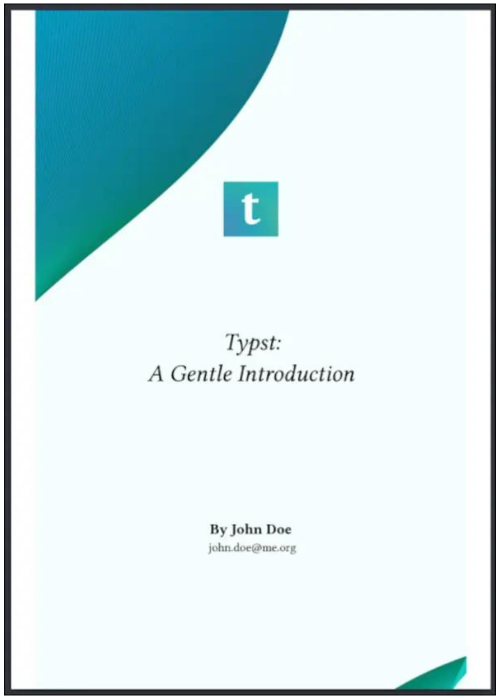
I encourage you to experiment with the "**Customize a template**" wizard and see the different layouts that you can generate. If you are writing a document that does not require a title page, you can place a headline-style title on the first page by choosing the option " **Title kind**: *Title row* ".

Title Page with Background Image

You can use the background parameter of Typst's page function to place content—such as a background image or a watermark—behind the page's body. This feature allows you to create some interesting graphic effects on your title page. In case you would like to try replicating these examples yourself, I uploaded the backgrounds and logos to a compressed archive in my personal Box.com account [9 images, 5.9 MB].

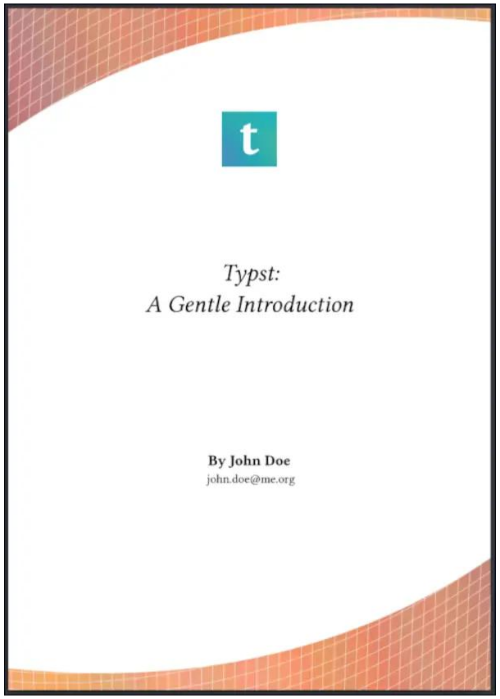
```
#set page(background: image("blue-
swoop-bkgd.jpg", width:
80%,),numbering:none)
#[
    #set align(center)
    #set text(30pt)
    #v(6cm)
    #image("typst-logo.png",width:15%)
    #v(3cm)
  _Typst: \ A Gentle Introduction_
  #v(5cm)
#set text(18pt)
*By John Doe* \
#set text(15pt)
#link("mailto: john.doe@me.org")
<pag-blue-swoop>
]

#set page(foreground: none, background:
none)
// This eliminates the background and
foreground for the rest
// of the document
```



Typst:
A Gentle Introduction

By John Doe
john.doe@me.org



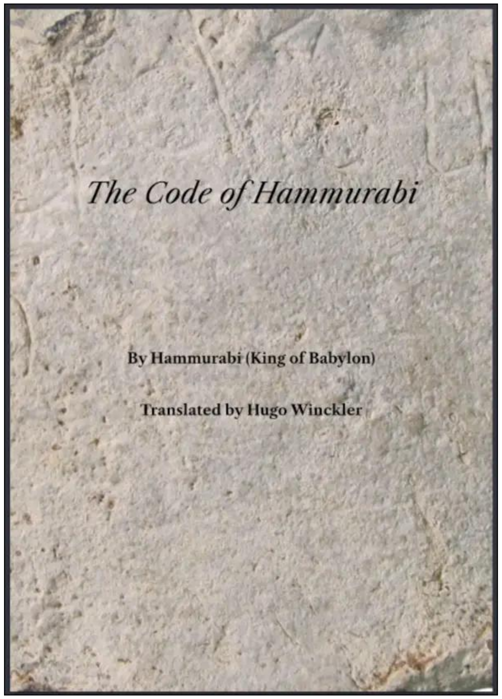
Typst:
A Gentle Introduction

By John Doe
john.doe@me.org

(Note: The second title page is a variant that uses an orange grid as the background.)

It is possible to set a photographic image as the background, if you wish. The background photo in the example below is a clay tablet. The typeface is Libre Caslon (released under the SIL Open Font License), which I downloaded from Font Squirrel and installed via the PCLinuxOS Control Center [PCC] (System menu > Manage, add and remove fonts > Import).

```
#set page(background: image("clay-
tablet.jpg", width:
210%,),numbering:none)
#[
#set align(center)
#set text(35pt, font: "Libre Caslon
Text")
#v(5cm)
_The Code of Hammurabi_
#v(5cm)
#set text(18pt, font: "Libre Caslon
Text")
*By Hammurabi (King of Babylon)*
#v(1cm)
*Translated by Hugo Winckler*
]
#set page(foreground: none, background:
none)
// This eliminates the background and
foreground for the rest
// of the document
```



The Code of Hammurabi

By Hammurabi (King of Babylon)

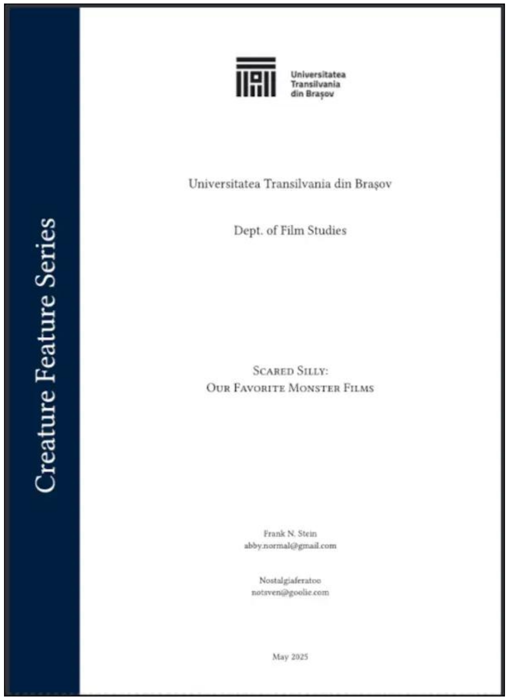
Translated by Hugo Winckler

Title Page with #grid()

ToniGL68 designed a nice title page using Typst's grid function, which he published in his Typst: Primeros pasos handbook (p. 30–32). Such wizardry is beyond my skill set, so I am grateful to him for creating this layout. With some trial and error, I was able to slightly modify the template to suit my needs.

```
#set page(margin: (x:0mm, y:0mm))

#grid( columns: (3cm,1fr), rows:
1fr, //stroke:1pt +red,
grid.cell(fill: navy)[
#align(center+horizon)[#text(fill:
white,35pt)[#rotate(-90deg,reflow:
true)[Creature Feature Series]]]
],
[#grid(columns: 1fr, rows:
(6cm,3cm,1cm,1fr,2cm,2cm,4cm),//stroke:
1pt+purple,
align(center+horizon)[#image("logo_ro-
RO.png",height: 31%)],
align(center+horizon)[#text(16pt)
[Universitatea Transilvania din
Bra ov]],
align(center+horizon)[#text(16pt)[Dept.
of Film Studies]],
align(center+horizon)[#text(16pt)
[#smallcaps[Scared Silly: \
Our Favorite Monster Films]]],
align(center+horizon)[Frank N. Stein \
#link("mailto:abby.normal@gmail.com")],
align(center+horizon)[Nostalgiaferatoo
\
#link("mailto:notsven@goolie.com")],
align(center+horizon)[May 2025]
)]
)
#pagebreak()
```



Creature Feature Series

Universitatea Transilvania din Brașov

Universitatea Transilvania din Brașov

Dept. of Film Studies

Scared Silly:
Our Favorite Monster Films

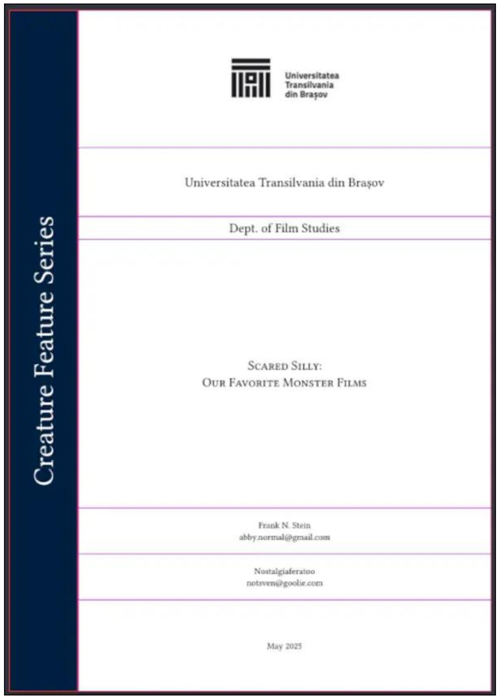
Frank N. Stein
abby.normal@gmail.com

Nostalgiaferatoo
notsven@goolie.com

May 2025

By adding a color stroke/line, we can better visualize the page's grid structure:

```
#set page(margin: (x:0mm, y:0mm))
#grid( columns: (3cm,1fr), rows: 1fr,
stroke:2pt +red,
grid.cell(fill: navy)[
    #align(center+horizon)[#text(fill:
white,35pt)[#rotate(-90deg,reflow:
true)[Creature Feature Series]]]
],
[#grid(columns: 1fr, rows:
(6cm,3cm,1cm,1fr,2cm,2cm,4cm),stroke:
1pt+purple,
align(center+horizon)[#image("logo_ro-
RO.png",height: 31%)],
[ . . . ]
```



Creature Feature Series

Universitatea Transilvania din Brașov

Dept. of Film Studies

Scared Silly:
Our Favorite Monster Films

Frank N. Stein
abby.normal@gmail.com

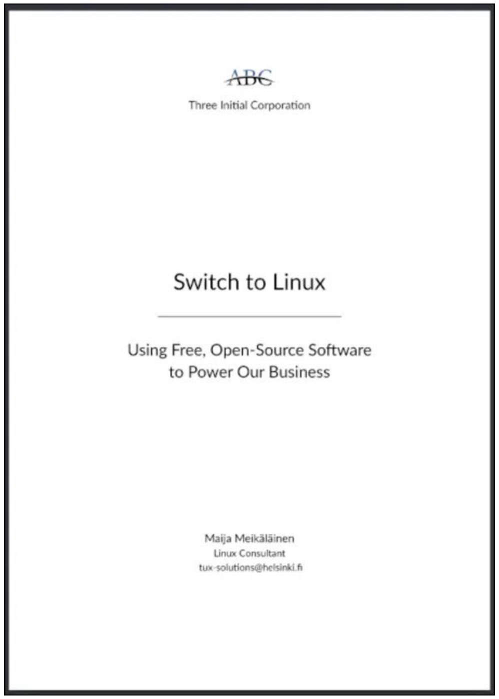
Nostalgiaferatoo
notsven@goolie.com

May 2025

Title Page with Simple Layout

The example below uses a plain block layout. Its major feature is a horizontal rule that separates the document title from the (smaller) subtitle. The heading area crisply displays the business name and its logo. The author information is shown at the bottom of the page, in a small block.

```
#set page(numbering:none)
#[
    #set align(center)
    #set text(14pt, font: "Lato")
    #image("logo-generic-
abc.png",width:15%)
    Three Initial Corporation
    #set text(28pt, font: "Lato")
    #v(6cm)
Switch to Linux
#line(length: 50%)
#set text(20pt, font: "Lato")
Using Free, Open-Source Software \ to
Power Our Business
   #v(6cm)
#set text(14pt, font: "Lato")
Maija Meikäläinen \
#set text(12pt)
Linux Consultant \
#link("mailto: tux-
solutions@helsinki.fi")
]
```



Three Initial Corporation

Switch to Linux

Using Free, Open-Source Software
to Power Our Business

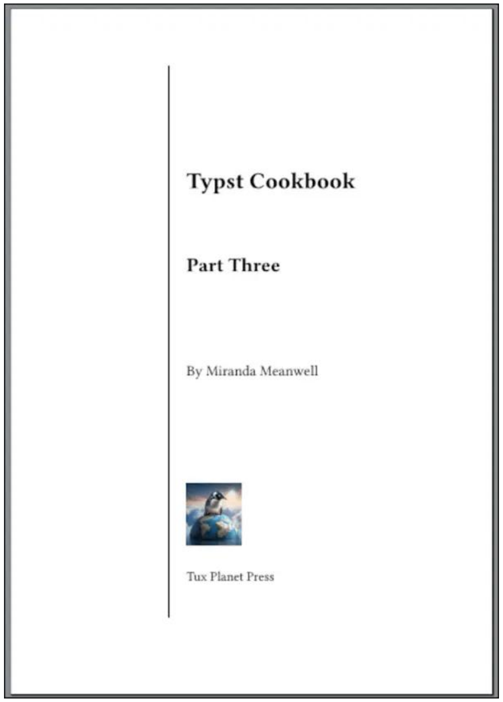
Maija Meikäläinen
Linux Consultant
tux-solutions@helsinki.fi

Title Page with Vertical Rule

This title page attempts to replicate the example given in Peter Wilson's booklet (p. 15). The design is asymmetrical, but the elements are aligned along a vertical rule, which helps guide the reader's attention. The grid layout is a modified version of a structure posted by user PgBiel in the Typst forum.

```
#grid(
    columns: (1fr, 0pt, 3fr),
    column-gutter: 2em,
    v(12em), [], v(3em),
    block(width: 100%, height: 3em,
stroke: none),
    grid.vline(stroke: 0.5pt),
    [],
    block(width: 100%, height: 5em,
text(28pt)[*Typst Cookbook*]),
    v(4.5em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: none),
    grid.vline(stroke: 2pt),
    [],
    block(width: 100%, height: 5em,
text(24pt)[*Part Three*]),

    v(7em), [], v(3em),
    block(width: 100%, height: 3em,
stroke: none),
    grid.vline(stroke: 0.5pt),
    [],
    block(width: 100%, height: 5em,
text(18pt)[By Miranda Meanwell]),
    v(8em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: none),
    grid.vline(stroke: 2pt),
    [],
    align(left+horizon)
[#image("penguin-atop-earth-sm'er.png",height: 11%)],
   v(3em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: none),
    grid.vline(stroke: 2pt),
    [],
    block(width: 100%, height: 5em,
text(16pt)[Tux Planet Press],
)
)
#pagebreak()
```



Typst Cookbook

Part Three

By Miranda Meanwell

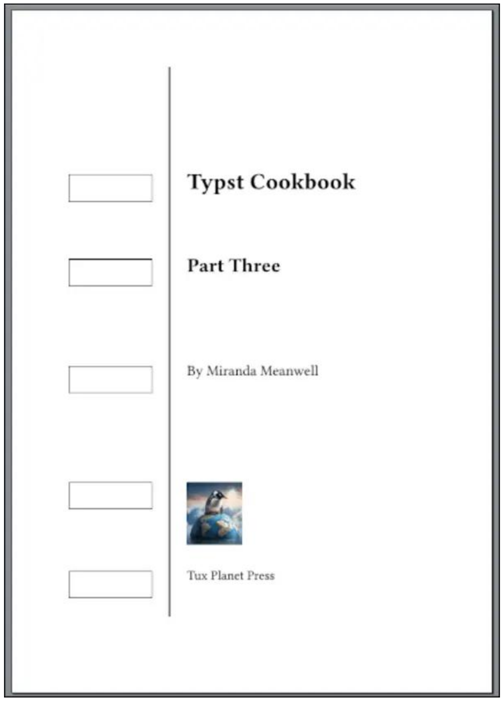
Tux Planet Press

By placing a stroke/line with a 1-point thickness around the block element, we can visualize the page's grid structure more clearly:

```
#grid(
    columns: (1fr, 0pt, 3fr),
    column-gutter: 2em,
    v(12em), [], v(3em),
    block(width: 100%, height: 3em,
stroke: 1pt),
    grid.vline(stroke: 0.5pt),
    [],
    block(width: 100%, height: 5em,
text(28pt)[*Typst Cookbook*]),
    v(4.5em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: 1pt),
    grid.vline(stroke: 2pt),
    [],
    block(width: 100%, height: 5em,
text(24pt)[*Part Three*]),

    v(7em), [], v(3em),
    block(width: 100%, height: 3em,
stroke: 1pt),
    grid.vline(stroke: 0.5pt),
    [],
    block(width: 100%, height: 5em,
text(18pt)[By Miranda Meanwell]),
    v(8em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: 1pt),
    grid.vline(stroke: 2pt),
    [],

    align(left+horizon)
[#image("penguin-atop-earth-sm'er.png",height: 11%)],
    v(3em),[],v(3em),
    block(width: 100%, height: 3em,
stroke: 1pt),
    grid.vline(stroke: 2pt),
    [],
    block(width: 100%, height: 5em,
text(16pt)[Tux Planet Press],
)
)
#pagebreak()
```



Typst Cookbook

Part Three

By Miranda Meanwell

Tux Planet Press

Fauxreilly Package

O'Reilly Media is famous for the animals on its tech book covers. Their distinctive design is immediately recognizable and has become part of the publisher's branding. A subpage of their website lets you sort books alphabetically by the name of the cover animal.

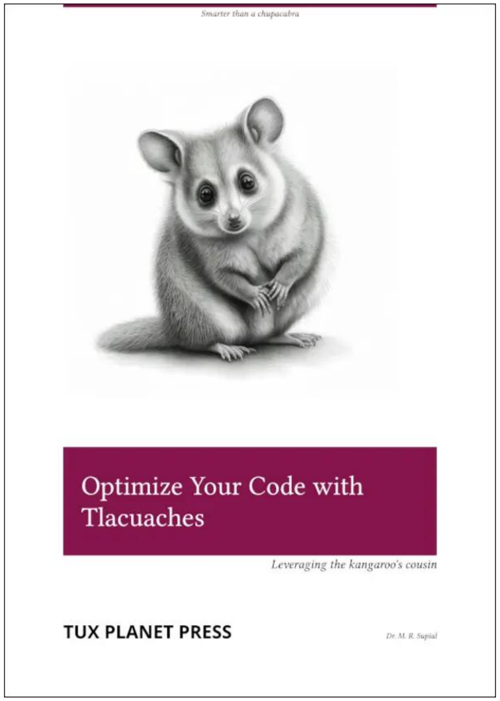
Typst user Dei Laborer wrote a clever package called *fauxreilly* for creating O'Reilly-style cover pages. Although it is limited to niche use cases, you might enjoy experimenting with it.

After importing the *fauxreilly* package into your Typst document, the sample code below produces the output shown in the screenshot. (Note: I changed the default publisher from "O RLY?" to "Tux Planet Press" by inserting the " publisher: " line.)

```
#import "@preview/fauxreilly:0.1.1": *
#orly(
    color: rgb("#85144b"),
    title: "Optimize Your Code with Tlacuaches",
    top-text: "Smarter than a chupacabra",
    subtitle: "Leveraging the kangaroo's cousin",
    publisher: "TUX PLANET PRESS",
    pic: image("possum-ai.jpg", width: 90%, fit: "contain"),
    signature: "Dr. M. R. Supial"
)
```

More Design Ideas

For more ideas about possible title page layouts, Peter Wilson's "Some Examples of Title Pages" (2010) is available via CTAN. It displays forty different designs of title pages taken from a selection of books and theses (using a variety of colors and fonts). Wilson's background includes engineering, physics and computer science; in the TeX world he is perhaps best known for having written LaTeX's memoir class.



Smarter than a chupacabra

Optimize Your Code with Tlacuaches

Leveraging the kangaroo's cousin

TUX PLANET PRESS

Dr. M. R. Supial

Additional Resources

Bringhurst, Robert. *The Elements of Typographic Style*. 3rd ed. Point Roberts, Wash.: Hartley & Marks, 2004.

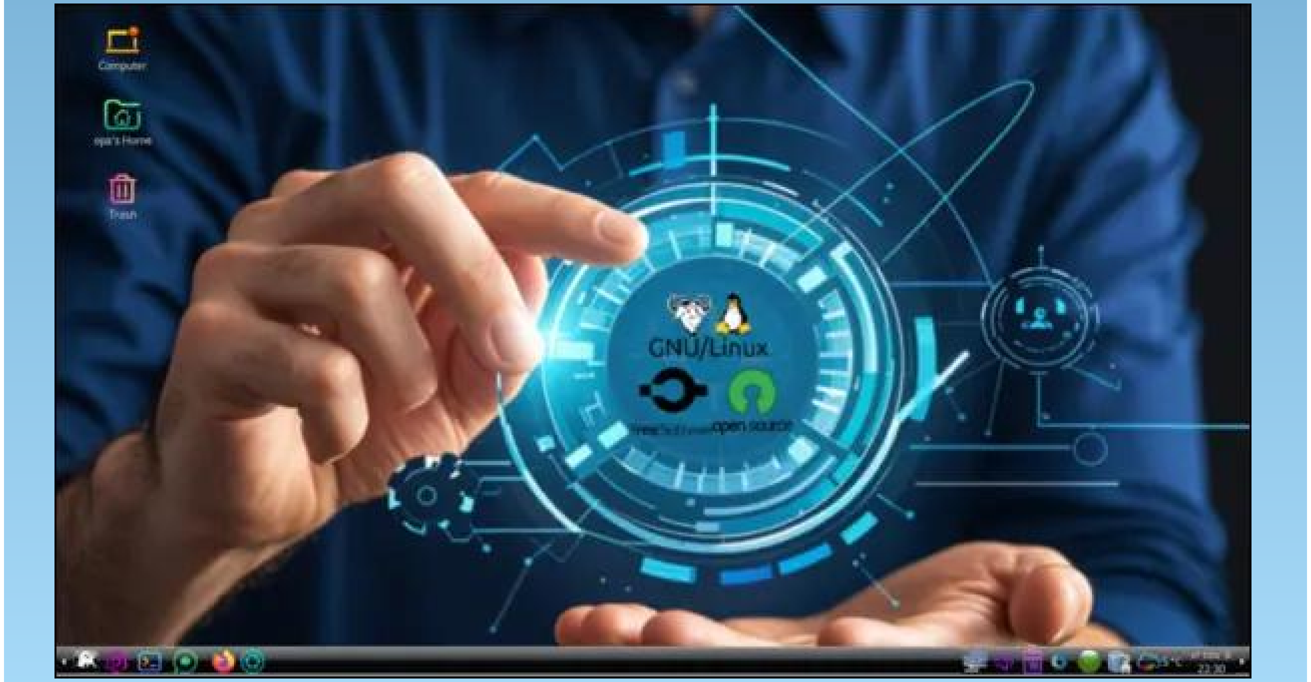
A classic work, which type designers Jonathan Hoefler and Tobias Frere-Jones consider to be "the finest book ever written about typography." Bringhurst's style is a bit florid, but he is a passionate expert who loves to share his knowledge.

Butterick, Matthew. *Butterick's Practical Typography*. 2nd ed. https://practicaltypography.com/

A good introduction for beginners. An online book that is ad-free and (voluntarily) supported by reader donations. If you do not have time to read the whole book, I suggest reviewing his basics and his summary of key rules.

I hope these examples will provide you with some practical templates, if you need to create a title page with Typst. If you would like to see a Typst-generated replica of this article, I have publicly shared my project from the web app. The document's body typeface is Source Serif Pro, and the headings use Source Sans Pro.

Screenshot Showcase



Posted by mutse, on November 8, 2024, running PCLOSDebian Mate.

How Cops Can Get Your Private Online Data

by Rory Mir and Aaron Mackey
Electronic Frontier Foundation

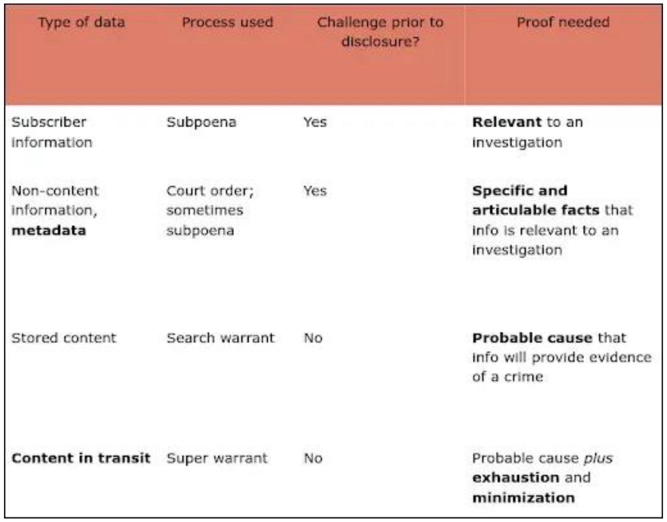
Can the cops get your online data? In short, yes. There are a variety of US federal and state laws which give law enforcement powers to obtain information that you provided to online services. But, there are steps you as a user and/or as a service provider can take to improve online privacy.

Law enforcement demanding access to your private online data goes back to the beginning of the internet. In fact, one of EFF's first cases, Steve Jackson Games v. Secret Service, exemplified the now all-too-familiar story where unfounded claims about illegal behavior resulted in overbroad seizures of user messages. But it's not the '90s anymore, the internet has become an integral part of everyone's life. Everyone now relies on organizations big and small to steward our data, from huge service providers like Google, Meta, or your ISP, to hobbyists hosting a blog or Mastodon server.

There is no "cloud," just someone else's computer—and when the cops come knocking on their door, these hosts need to be willing to stand up for privacy, and know how to do so to the fullest extent under the law. These legal limits are also important for users to know, not only to mitigate risks in their security plan when choosing where to share data, but to understand whether these hosts are going to bat for them. Taking action together, service hosts and users can curb law enforcement getting more data than they're allowed, protecting not just themselves but targeted populations, present and future.

This is distinct from law enforcement's methods of collecting public data, such as the information now being collected on student visa applicants. Cops may use social media monitoring tools and sock puppet accounts to collect what you share publicly, or even within "private" communities. Police may also obtain the contents of communication in other ways that do not require court authorization, such as monitoring network traffic passively to catch metadata and possibly using advanced tools to partially reveal encrypted information. They can even outright buy information from online data brokers. Unfortunately, there are few restrictions or oversight for these practices—something EFF is fighting to change.

Below, however is a general breakdown of the legal processes used by US law enforcement for accessing private data, and what categories of private data these processes can disclose. Because this is a generalized summary, it is neither exhaustive nor should be considered legal advice. Please seek legal help if you have specific data privacy and security needs.



Type of data	Process used	Challenge prior to disclosure?	Proof needed
Subscriber information	Subpoena	Yes	**Relevant** to an investigation
Non-content information, **metadata**	Court order; sometimes subpoena	Yes	**Specific and articulable facts** that info is relevant to an investigation
Stored content	Search warrant	No	**Probable cause** that info will provide evidence of a crime
Content in transit	Super warrant	No	Probable cause *plus* **exhaustion** and **minimization**

Types of Data that Can be Collected

The laws protecting private data online generally follow a pattern: the more sensitive the personal data is, the greater factual and legal burden police have to meet before they can obtain it. Although this is not exhaustive, here are a few categories of data you may be sharing with services, and why police might want to obtain it.

Subscriber Data: Information you provide in order to use the service. Think about ID or payment information, IP address location, email, phone number, and other information you provided when signing up. *Law enforcement can learn who controls an anonymous account, and find other service providers to gather information from.*

Non-content data, or "metadata": This is saved information about your interactions on the service; like when you used the service, for how long, and with whom. Analogous to what a postal worker can infer from a sealed letter with addressing information. *Law enforcement can use this information to infer a social graph, login history, and other information about a suspect's behavior.*

Stored content: This is the actual content you are sending and receiving, like your direct message history or saved drafts. This can cover any private information your service provider can access. *This most sensitive data is collected to reveal criminal evidence. Overly broad requests also allow for retroactive searches, information on other users, and can take information out of its original context.*

Content in transit: This is the content of your communications as it is being communicated. This real-time access may also collect info which isn't typically stored by a provider, like your voice during a phone call. *Law enforcement can compel providers to wiretap their own services for a particular user—which may also implicate the privacy of users they interact with.*

Legal Processes Used to Get Your Data

When US law enforcement has identified a service that likely has this data, they have a few tools to legally compel that service to hand it over and prevent users from knowing information is being collected.

Subpoena

Subpoenas are demands from a prosecutor, law enforcement, or a grand jury which do not require approval of a judge before being sent to a service. The only restriction is this demand be relevant to an investigation. Often the only time a court reviews a subpoena is when a service or user challenges it in court.

Due to the lack of direct court oversight in most cases, subpoenas are prone to abuse and overreach. Providers should scrutinize such requests carefully with a lawyer and push back before disclosure, particularly when law enforcement tries to use subpoenas to obtain more private data, such as the contents of communications.

Court Order

This is a similar demand to subpoenas, but usually pertains to a specific statute which requires a court to authorize the demand. Under the Stored Communications Act, for example, a court can issue an order for non-content information if police provide specific facts that the information being sought is relevant to an investigation.

Like subpoenas, providers can usually challenge court orders before disclosure and inform the user(s) of the request, subject to law enforcement obtaining a gag order (more on this below).

Search Warrant

A warrant is a demand issued by a judge to permit police to search specific places or persons. To obtain a warrant, police must submit an affidavit (a written statement made under oath) establishing that there is a fair probability (or "probable cause") that evidence of a crime will be found at a particular place or on a particular person.

Typically, services cannot challenge a warrant before disclosure, as these requests are already approved by a magistrate. Sometimes police request that judges also enter gag orders against the target of the warrant that prevent hosts from informing the public or the user that the warrant exists.

Super Warrant

Police seeking to intercept communications as they occur generally face the highest legal burden. Usually, the affidavit needs to not only establish probable cause, but also make clear that other investigation methods are not viable (exhaustion) and that the collection avoids capturing irrelevant data (minimization).

Some laws also require high-level approval within law enforcement, such as leadership, to approve the request. Some laws also limit the types of crimes that law enforcement may use wiretaps in while they are investigating. The laws may also require law enforcement to periodically report back to the court about the wiretap, including whether they are minimizing collection of non-relevant communications.

Generally, these demands cannot be challenged while wiretapping is occurring, and providers are prohibited from telling the targets about the wiretap. But some laws require disclosure to targets and those who were communicating with them after the wiretap has ended.

Gag orders

Many of the legal authorities described above also permit law enforcement to simultaneously prohibit the service from telling the target of the legal process or the general public that the surveillance is occurring. These non-disclosure orders are prone to abuse and EFF has repeatedly fought them because they violate the First Amendment and prohibit public understanding about the breadth of law enforcement surveillance.

How Services Can (and Should) Protect You

This process isn't always clean-cut, and service providers must ultimately comply with lawful demands for user's data, even when they challenge them and courts uphold the government's demands.

Service providers outside the US also aren't totally in the clear, as they must often comply with US law enforcement demands. This is usually because they either have a legal presence in the US or because they can be compelled through mutual legal assistance treaties and other international legal mechanisms.

However, services can do a lot by following a few best practices to defend user privacy, thus limiting the impact of these requests and in some cases make their service a less appealing door for the cops to knock on.

Put Cops through the Process

Paramount is the service provider's willingness to stand up for their users. Carving out exceptions or volunteering information outside of the legal framework erodes everyone's right to privacy. Even in extenuating and urgent circumstances, the responsibility is not on you to decide what to share, but on the legal process.

Smaller hosts, like those of decentralized services, might be intimidated by these requests, but consulting legal counsel will ensure requests are challenged when necessary. Organizations like EFF can sometimes provide legal help directly or connect service providers with alternative counsel.

Challenge Bad Requests

It's not uncommon for law enforcement to overreach or make burdensome requests. Before offering information, services can push back on an improper demand informally, and then continue to do so in court. If the demand is overly broad, violates a user's First or Fourth Amendment rights, or has other legal defects, a court may rule that it is invalid and prevent disclosure of the user's information.

Even if a court doesn't invalidate the legal demand entirely, pushing back informally or in court can limit how much personal information is disclosed and mitigate privacy impacts.

Provide Notice

Unless otherwise restricted, service providers should give notice about requests and disclosures as soon as they can. This notice is vital for users to seek legal support and prepare a defense.

Be Clear With Users

It is important for users to understand if a host is committed to pushing back on data requests to the full extent permitted by law. Privacy policies with fuzzy thresholds like "when deemed appropriate" or "when requested" make it ambiguous if a user's right to privacy will be respected. The best practices for providers not only require clarity and a willingness to push back on law enforcement demands, but also a commitment to be transparent with the public about law enforcement's demands. For example, with regular transparency reports breaking down the countries and states making these data requests.

Social media services should also consider clear guidelines for finding and removing sock puppet accounts operated by law enforcement on the platform, as these serve as a backdoor to government surveillance.

Minimize Data Collection

You can't be compelled to disclose data you don’t have. If you collect lots of user data, law enforcement will eventually come demanding it. Operating a service typically requires some collection of user data, even if it’s just login information. But the problem is when information starts to be collected beyond what is strictly necessary.

This excess collection can be seen as convenient or useful for running the service, or often as potentially valuable, like behavioral tracking used for advertising. However, the more that’s collected, the more the service becomes a target for both legal demands and illegal data breaches.

For data that enables desirable features for the user, design choices can make privacy the default and give users additional (preferably opt-in) sharing choices.

Shorter Retention

As another minimization strategy, hosts should regularly and automatically delete information when it is no longer necessary. For example, deleting logs of user activity can limit the scope of law enforcement’s retrospective surveillance—maybe limiting a court order to the last 30 days instead of the lifetime of the account.

Again, design choices, like giving users the ability to send disappearing messages and deleting them from the server once they’re downloaded, can also further limit the impact of future data requests. Furthermore, these design choices should have privacy-preserving default

Avoid Data Sharing

Depending on the service being hosted there may be some need to rely on another service to make everything work for users. Third-party login or ad services are common examples with some amount of tracking built in. Information shared with these third-parties should also be minimized and avoided, as they may not have a strict commitment to user privacy. Most notoriously, data brokers who sell advertisement data can provide another legal work-around for law enforcement by letting them simply buy collected data across many apps. This extends to decisions about what information is made public by default, thus accessible to many third parties, and if that is clear to users.

(True) End-to-End Encryption

Now that HTTPS is actually everywhere, most traffic between a service and a user can be easily secured—for free. This limits what onlookers can collect on users of the service, since messages between the two are in a secure “envelope.” However, this doesn’t change the fact the service is opening this envelope before passing it along to other users, or returning it to the same user. With each opened message, this is more information to defend.

Better, is end-to-end encryption (e2ee), which just means providing users with secure envelopes that even the service provider cannot open. This is how a featureful messaging app like Signal can respond to requests with only three pieces of information: the account identifier (phone number), the date of creation, and the last date of access. Many services should follow suit and limit access through encryption.

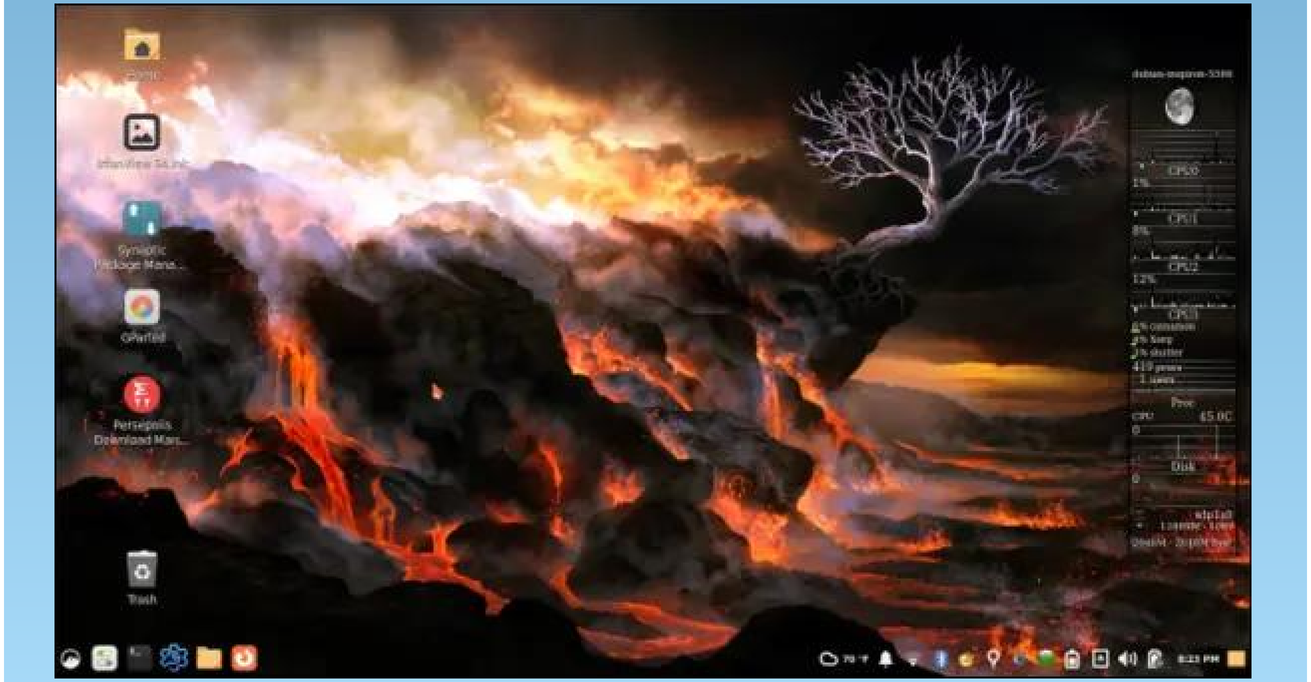
Note that while e2ee has become a popular marketing term, it is simply inaccurate for describing any encryption use designed to be broken or circumvented. Implementing “encryption backdoors” to break encryption when desired, or simply collecting information before or after the envelope is sealed on a user’s device (“client-side scanning”) is antithetical to encryption. Finally, note that e2ee does not protect against law enforcement obtaining the contents of communications should they gain access to any device used in the conversation, or if message history is stored on the server unencrypted.

Protecting Yourself and Your Community

As outlined, often the security of your personal data depends on the service providers you choose to use. But as a user you do still have some options. EFF’s Surveillance Self-Defense is a maintained resource with many detailed steps you can take. In short, you need to assess your risks, limit the services you use to those you can trust (as much as you can), improve settings, and when all else fails, accessorize with tools that prevent data sharing in the first place —like EFF's Privacy Badger browser extension.

Remember that privacy is a team sport. It's not enough to make these changes as an individual, it's just as important to share and educate others, as well as fighting for better digital privacy policy on all levels of governance. Learn, get organized, and take action.

Screenshot Showcase



Posted by Nish, on May 28, 2024, running PCLOSDebian-Cinnamon.

GIMP 3.0 Review

by Meemaw

GIMP Splash

GIMP 3.0.4 is out! As I reported earlier, the packagers were having trouble with the program, but put the appimage in the repo. I decided not to review it until their problems were resolved. My preference only. With the release of version 3.0.4, we have it in the repo rather than an appimage, and I can review some of the new features and fixes. I used the following sites in my exploration: librearts.org, the GIMP Manual, and creativeblog.com.

New Welcome Screen

GIMP has always opened onto your program window, ready to start a project, or onto whatever you opened to work on. Now it has a welcome screen consisting of five tabs:

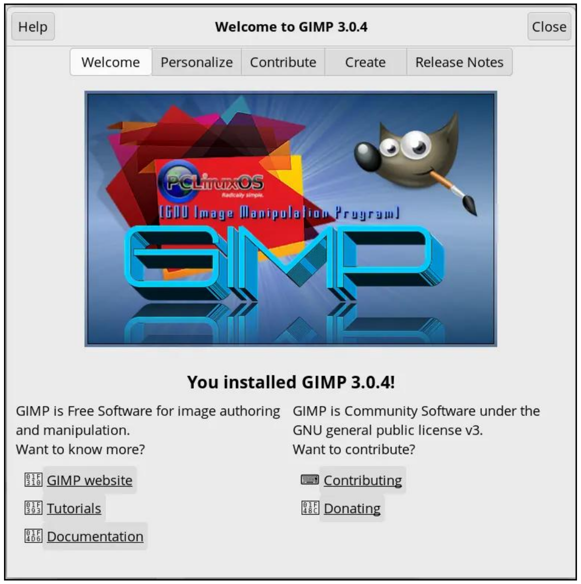
Welcome has the splash screen (ours is one for PCLOS) and several helpful links.

Personalize has some of the basic edits for appearance, so you can get started right away.

Contribute has links to help you contribute to development.

Create has a list of your recent projects, a "Create New Image" button and an "Open Existing Image" button. It also has a checkbox at the bottom to turn off the welcome screen if desired.

Release Notes lists some of the new features, with a "flash" effect on some that will show you where they are (not included below).



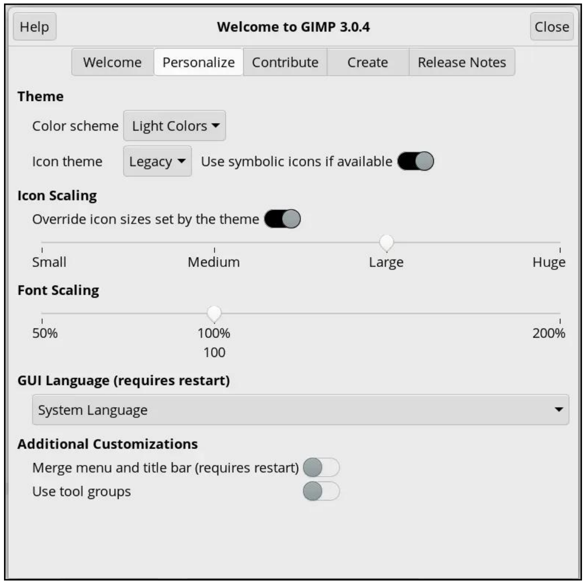
You installed GIMP 3.0.4!

GIMP is Free Software for image authoring and manipulation.
Want to know more?

- GIMP website
- Tutorials
- Documentation

GIMP is Community Software under the GNU general public license v3.
Want to contribute?

- Contributing
- Donating



Theme

Color scheme: Light Colors

Icon theme: Legacy — Use symbolic icons if available

Icon Scaling

Override icon sizes set by the theme

Small — Medium — Large — Huge

Font Scaling

50% — 100% — 200%

100

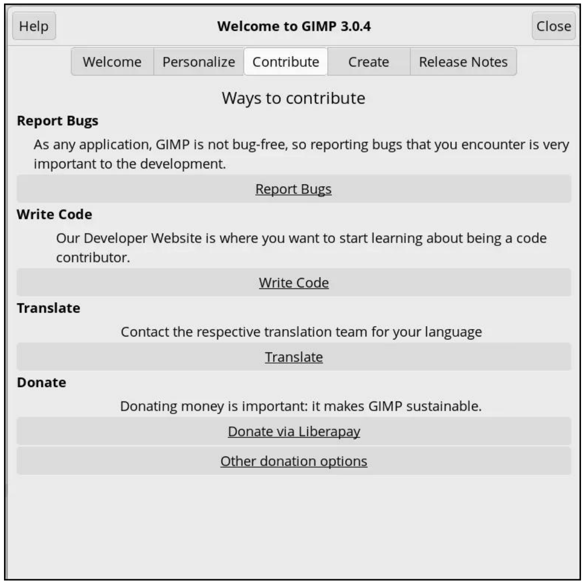
GUI Language (requires restart)

System Language

Additional Customizations

Merge menu and title bar (requires restart)

Use tool groups



Ways to contribute

Report Bugs

As any application, GIMP is not bug-free, so reporting bugs that you encounter is very important to the development.

Report Bugs

Write Code

Our Developer Website is where you want to start learning about being a code contributor.

Write Code

Translate

Contact the respective translation team for your language

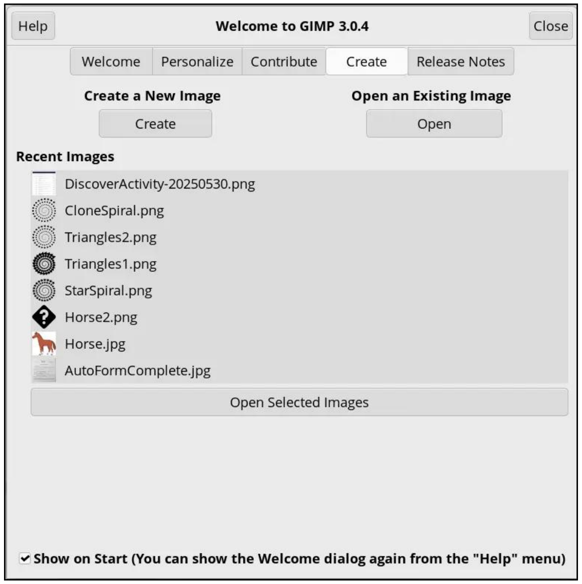
Translate

Donate

Donating money is important: it makes GIMP sustainable.

Donate via Liberapay

Other donation options



Help | Welcome to GIMP 3.0.4 | Close

Welcome | Personalize | Contribute | Create | Release Notes

Create a New Image

Create

Open an Existing Image

Open

Recent Images

- DiscoverActivity-20250530.png
- CloneSpiral.png
- Triangles2.png
- Triangles1.png
- StarSpiral.png
- Horse2.png
- Horse.jpg
- AutoFormComplete.jpg

Open Selected Images

☑ Show on Start (You can show the Welcome dialog again from the "Help" menu)

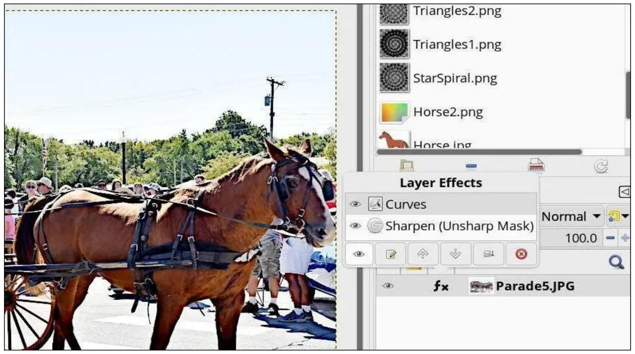
Non-Destructive Editing

(From creativeblog.com) “One of the most asked for features/workflows arrives in this release with additional updates. Non-Destructive Editing (NDE) appeared in a recent previous release, and is now being further refined. This is of course a very important addition, and allows attributes like Levels and other modifications to be applied, and later either removed or adjusted at will.

You will see a small “fx” icon next to the layer in the Layer Pallet. When clicked, it brings up options to turn the effect on/off, modify or delete. A “Merge filter” toggle will flatten the layer effects.”

(From the release notes) “In GIMP 2.10, filters were automatically merged onto the layer, which prevented you from making further edits without repeatedly undoing your changes. Now, by default, filters stay active once committed. This means you can re-edit most GEGL filters in the fx menu on the layer dockable without having to revert your work.”

When you edit something, any effect you use, including color edits, are added to the layer window on the layer you are editing, and you can see the edits on your image. I opened the following image and used the Unsharp Mask filter and then edited the colors using Curves. As you can see in the second photo, when I click the *fx* to the left of the layer, those two operations are in the layer effects.



Those effects can be moved up and down in the layer effects dialog (all in the layers), which could possibly change the way your image looks. Saving your project as an xcf file preserves all of this. It’s only when you finally export your project that the effects are merged into the layer. Most of the effects are now non-destructive, according to the GIMP release notes. Most of the GEGL filters are non-destructive, but some of the others are not. They recommend you search the filters to see which ones are GEGL.

Something I noticed right away — when you copy and paste something, GIMP puts it on a NEW layer, rather than a FLOATING layer. You can anchor it using Merge Down. You can also use the menu item Paste as Floating Layer, then merge down.

Layer Groups

“Layer Groups” enable you to group layers together in a hierarchical structure. This will make it easier to manage your project if you have many layers.

Create a Layer Group

You can create a layer group by clicking the **New Layer Group** button at the bottom of the Layers Dialog (it looks like a folder), by using the menu command **Layer > New Layer Group**, or through the right click Layers context menu.

You'll see the new layer group above the layer you selected earlier. You should give it a descriptive name so you know what that group is. You rename it exactly the same way you rename layers.

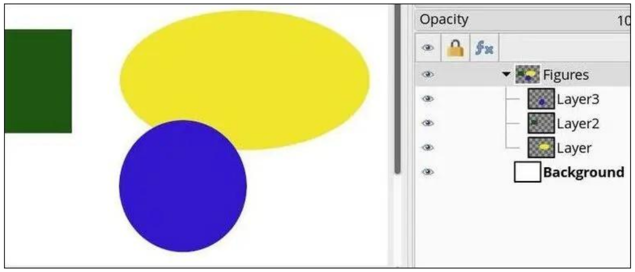
You can create multiple layer groups, and you can **embed** them, that is, include a layer group inside another group.

Adding Layers to a Layer Group

You can add existing layers to a layer group by click-and-dragging them. If you want more than one layer in that group, select them all and drag them into the group.

To add a new layer to the current layer group, select the New Layer Group where you want your new layer to be, then click the New Layer button. An Add Layer window will appear, just as always.

When a layer group is not empty, a small triangular icon appears. By clicking it, you can open or close the group.

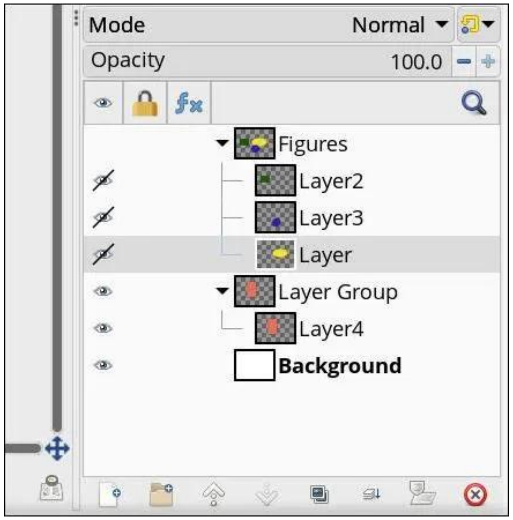

Opacity 10

Layers that belong to a layer group are slightly indented to the right, allowing you to easily see which layers are part of the group.

From the GIMP Manual:

If a layer group is made invisible using the eye icon but still open (so that the layers inside the group are shown in the list), there is a struck out eye shown besides the layers that are inside the group to indicate that these layers are not displayed in the final projection of the image, but theoretically visible in the layer group.

In this example, I clicked the "eye" in front of the top layer group, and everything in that layer group is not visible now. However, you can see the crossed-out eyes in front of the individual layers.


Mode Normal
Opacity 100.0

Also from the GIMP Manual:

Opacity

When a layer group is activated, opacity changes are applied to all the layers of the group.

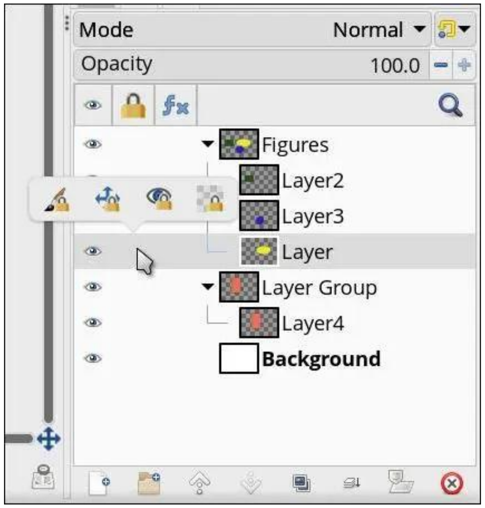
Layer Mask

Masks are also available on layer groups. They work similarly to ordinary layer masks, with the following considerations.

The layer group's mask size is the same as the combined size of all its children at all times. When the group's size changes, the mask is cropped to the new size — areas of the mask that fall outside of the new bounds are discarded, and newly added areas are filled with black (and hence are transparent by default).

Layer Locks

The various locks for layers have moved from the toolbar above the layers tree view to the layer rows. Click where a lock icon is supposed to be visible in the Lock column and select the options you need. Below, I clicked on the space that had the square for the layer lock and got this:


Mode Normal
Opacity 100.0

You'll see four icons. From left to right: Lock pixels, lock position and size, lock visibility, and lock Alpha channel. Choose the one that you need.

Text Outline

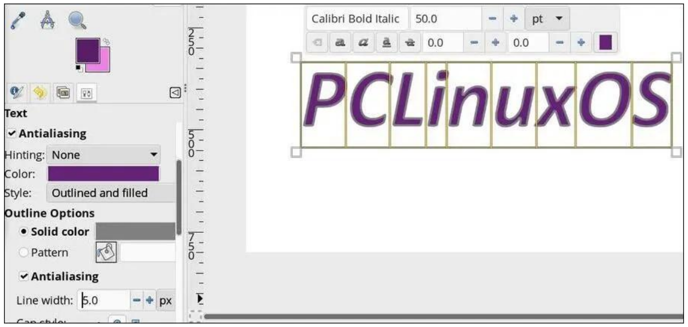
The **Text** tool has two new styles: **Outlined** and **Outlined and filled**. It does what it says in the text tool. However, librearts reported that the rendering quality is not amazing, and the *UI is kind of clunky*. In fact, I tried to put some text on a layer, and while choosing the colors, GIMP crashed on the setting Outlined and Filled. I have seen several bug reports submitted to GIMP, so I'm sure they are working on it. Editing the text is possible, and the fill defaults to your foreground color, but the default outline is gray, and trying to choose a different color for the outline is where the program crashes.

I was, however, able to change the outline from 10 px to 5 px, and the color of the fill to green and then purple. If you're willing to leave the outline color gray, the rest of it still works. It's just that the outline color stays gray, even on the Outlined setting, and attempts to change it crashes GIMP (center, top).

More to See!

Wilbur has a new design! They updated/modernized the Wilbur icon.

Additional export formats were added, including psd for Photoshop, in case you need to share.



Text
✓ Antialiasing
Hinting: None
Color:
Style: Outlined and filled
Outline Options
● Solid color
○ Pattern
✓ Antialiasing
Line width: 5.0 px

Calibri Bold Italic 50.0 pt
0.0 0.0

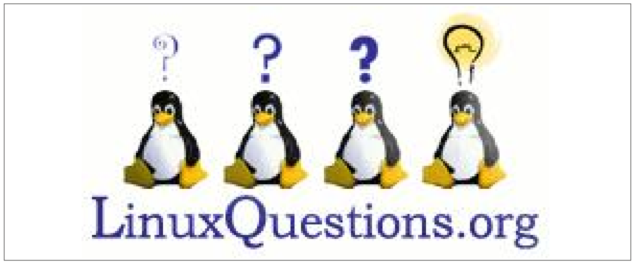
Fonts are more accurately stored and displayed.

Updated translations: GIMP is available in 85 languages, and 47 of them have been updated.

In **Preferences** > **Canvas Interaction** > **Modifiers**, you can customize actions you want your mouse buttons to perform with a specific tool.

New (Experimental) Tool: The new tool (Paint Select) allows progressive selection using a brush. However, it is very unstable, so is only included in the Playground section of the Preferences dialog. That is only visible if you run GIMP with the —*show-playground* flag.

I don't think this is everything, but it will get you started, if you haven't explored yet.



FBI Warning On IoT Devices: How To Tell If You Are Impacted

by Alexis Hancock and Bill Budington
Electronic Frontier Foundation

On June 5th, the FBI released a PSA titled "Home Internet Connected Devices Facilitate Criminal Activity." This PSA largely references devices impacted by the latest generation of BADBOX malware (as named by HUMAN's Satori Threat Intelligence and Research team) that EFF researchers also encountered primarily on Android TV set-top boxes. However, the malware has impacted tablets, digital projectors, aftermarket vehicle infotainment units, picture frames, and other types of IoT devices.

One goal of this malware is to create a network proxy on the devices of unsuspecting buyers, potentially making them hubs for various potential criminal activities, putting the owners of these devices at risk from authorities. This malware is particularly insidious, coming pre-installed out of the box from major online retailers such as Amazon and AliExpress. If you search "Android TV Box" on Amazon right now, many of the same models that have been impacted are still up being sold by sellers of opaque origins. Facilitating the sale of these devices even led us to write an open letter to the FTC, urging them to take action on resellers.

The FBI listed some indicators of compromise (IoCs) in the PSA for consumers to tell if they were impacted. But the average person isn't running network detection infrastructure in their homes, and cannot hope to understand what IoCs can be used to determine if their devices generate "unexplained or suspicious Internet traffic." Here, we will attempt to help give more comprehensive background information about these IoCs. If you find any of these on devices you own, then we encourage you to follow through by contacting the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov.

The FBI lists these IoC:

- The presence of suspicious marketplaces where apps are downloaded.

- Requiring Google Play Protect settings to be disabled.

- Generic TV streaming devices advertised as unlocked or capable of accessing free content.

- IoT devices advertised from unrecognizable brands.

- Android devices that are not Play Protect certified.

- Unexplained or suspicious Internet traffic.

The following adds context to the above, as well as some added IoCs we have seen from our research.

Play Protect Certified

"Android devices that are not Play Protect certified" refers to any device brand or partner not listed here. Google subjects devices to compatibility and security tests in their criteria for inclusion in the Play Protect program, though the mentioned list's criteria are not made completely transparent outside of Google. But this list does change, as we saw with the tablet brand we researched being de-listed. This encompasses "devices advertised from unrecognizable brands." The list includes international brands and partners as well.

Outdated Operating Systems

Other issues we saw were really outdated Android versions. For posterity, Android 16 just started rolling out. Android 9-12 appeared to be the most common versions routinely used. This could be a result of "copied homework" from previous legitimate Android builds, and often come with their own update software that can present a problem on its own and deliver second-stage payloads for device infection in addition to what it is downloading and updating on the device.

You can check which version of Android you have by going to Settings and searching "Android version".

Android App Marketplaces

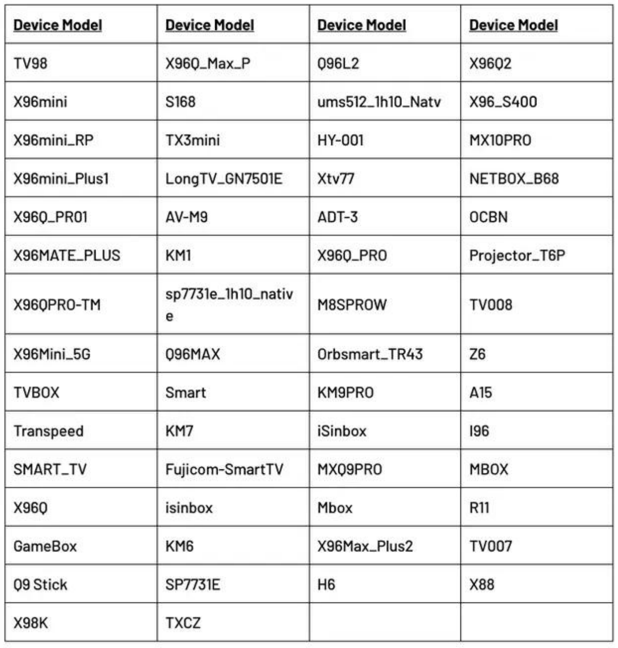
We've previously argued how the availability of different app marketplaces leads to greater consumer choice, where users can choose alternatives even more secure than the Google Play Store. While this is true, the FBI's warning about suspicious marketplaces is also prudent. Avoiding "downloading apps from unofficial marketplaces advertising free streaming content" is sound (if somewhat vague) advice for set-top boxes, yet this recommendation comes without further guidelines on how to identify which marketplaces might be suspicious for other Android IoT platforms. Best practice is to investigate any app stores used on Android devices separately, but to be aware that if a suspicious Android device is purchased, it can contain preloaded app stores that mimic the functionality of legitimate ones but also contain unwanted or malicious code.

Models Listed from the Badbox Report

We also recommend looking up device names and models that were listed in the BADBOX 2.0 report. We investigated the T95 models along with other independent researchers that initially found this malware present. A lot of model names could be grouped in families with the same letters but different numbers. These operations are iterating fast, but the naming conventions are often lazy in this respect. If you're not sure what model you own, you can usually find it listed on a sticker somewhere on the device. If that fails, you may be able to find it by pulling up the original receipt or looking through your order history.

A Note from Satori Researchers:

"Below is a list of device models known to be targeted by the threat actors. Not all devices of a given model are necessarily infected, but Satori researchers are confident that infections are present on some devices of the below device models:"



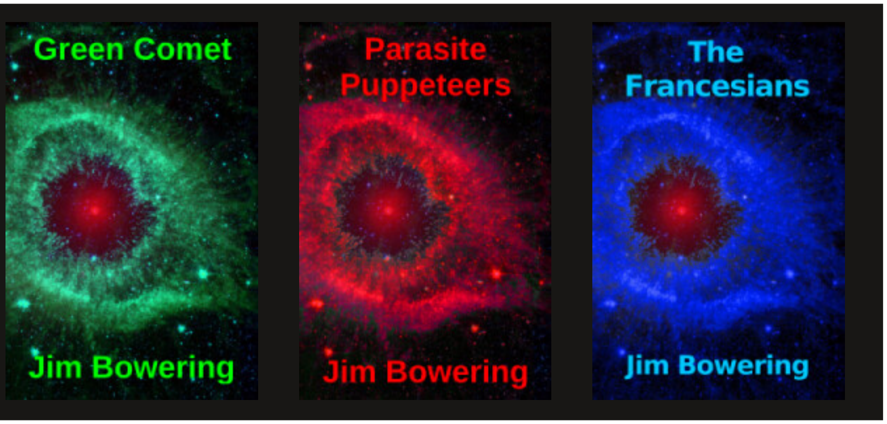
Device Model	Device Model	Device Model	Device Model
TV98	X96Q_Max_P	Q96L2	X96Q2
X96mini	S168	ums512_1h10_Natv	X96_S400
X96mini_RP	TX3mini	HY-001	MX10PRO
X96mini_Plus1	LongTV_GN7501E	Xtv77	NETBOX_B68
X96Q_PR01	AV-M9	ADT-3	OCBN
X96MATE_PLUS	KM1	X96Q_PRO	Projector_T6P
X96QPRO-TM	sp7731e_1h10_native	M8SPROW	TV008
X96Mini_5G	Q96MAX	Orbsmart_TR43	Z6
TVBOX	Smart	KM9PRO	A15
Transpeed	KM7	iSinbox	I96
SMART_TV	Fujicom-SmartTV	MXQ9PRO	MBOX
X96Q	isinbox	Mbox	R11
GameBox	KM6	X96Max_Plus2	TV007
Q9 Stick	SP7731E	H6	X88
X98K	TXCZ		

List of Potentially Impacted Models

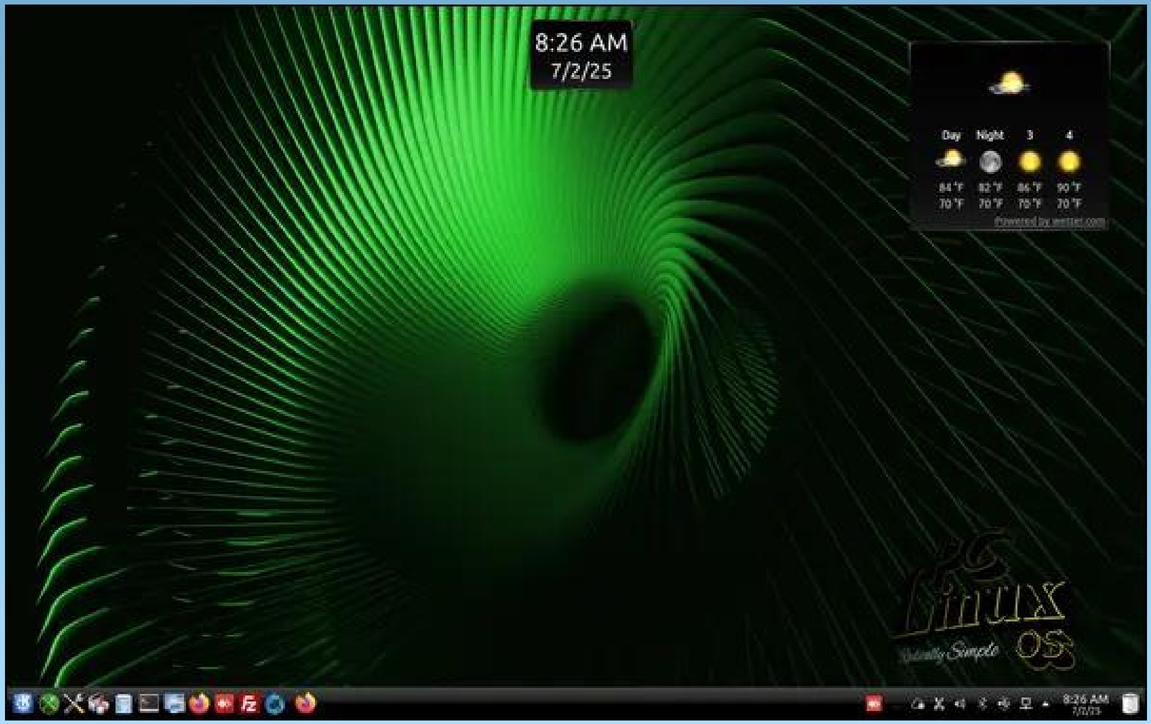
Broader Picture: The Digital Divide

Unfortunately, the only way to be sure that an Android device from an unknown brand is safe is not to buy it in the first place. Though initiatives like the U.S. Cyber Trust Mark are welcome developments intended to encourage demand-side trust in vetted products, recent shake ups in federal regulatory bodies means the future of this assurance mark is unknown. This means those who face budget constraints and have trouble affording top-tier digital products for streaming content or other connected purposes may rely on cheaper imitation products that are rife with not only vulnerabilities, but even come out-of-the-box preloaded with malware. This puts these people disproportionately at legal risk when these devices are used to provide the buyers' home internet connection as a proxy for nefarious or illegal purposes.

Cybersecurity and trust that the products we buy won't be used against us is essential: not just for those that can afford name-brand digital devices, but for everyone. While we welcome the IoCs that the FBI has listed in its PSA, more must be done to protect consumers from a myriad of dangers that their devices expose them to.



Screenshot Showcase



Posted by Ramchu, on July 2, 2025, running KDE.

Wiki Pick: Restore Grub2

by The PCLinuxOS Community

Relevant to all editions of PCLinuxOS.

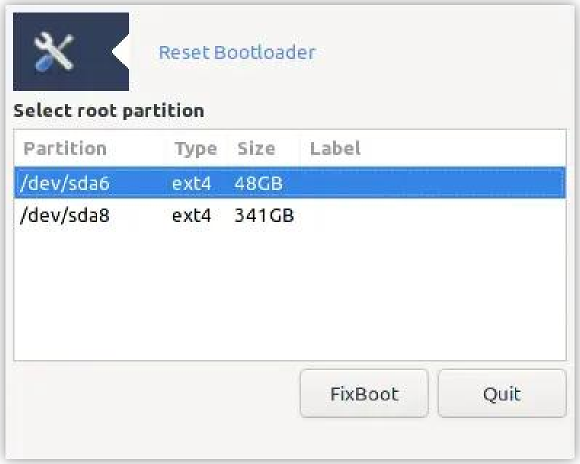
Your bootloader may end up corrupt or overwritten by another operating system due to many factors such as user error, power loss or malware etc. In such situations, you may find yourself in search of a way to restore your bootloader to a state in which it will normally load your favorite PCLinuxOS.

To fix or restore the GRUB2 bootloader on your PCLinuxOS system you will need to boot a recent PCLinuxOS LiveOS then you can choose one of the 2 methods below depending on whether you prefer using the command-line or graphical user interface.

Using redo-bootloader graphical tool

You will find the redo-bootloader application in the Configuration section of the main menu. If it is missing, then install the redo-bootloader package using the Synaptic package manager.

The window shows the Linux partitions available on your system. Select the correct root partition and then click FixBoot. The tool will then mount that partition and enable you to re-install the bootloader.



Select root partition

Partition	Type	Size	Label
/dev/sda6	ext4	48GB	
/dev/sda8	ext4	341GB	

Using the command-line interface

If you prefer to use the command line, then open a root terminal and enter the following commands:

```
mkdir -p /mnt
 mount /dev/sdaX /mnt
(replace sdaX with whatever your root partition is)
```

If this is a UEFI system mount the EFI System Partition (ignore this step for a BIOS/legacy system).

```
mount /dev/sdaY /mnt/boot/EFI
(replace sdaY with whatever your ESP is)
```

Run the following commands to re-install the grub bootloader code:

```
for i in /sys /proc /dev; do mount -B $i /mnt$i; done

chroot /mnt /boot/grub2/install.sh
```

If all goes well, you will see:

```
Installation finished. No error reported.
```

Exit the chroot environment with CTRL-D.

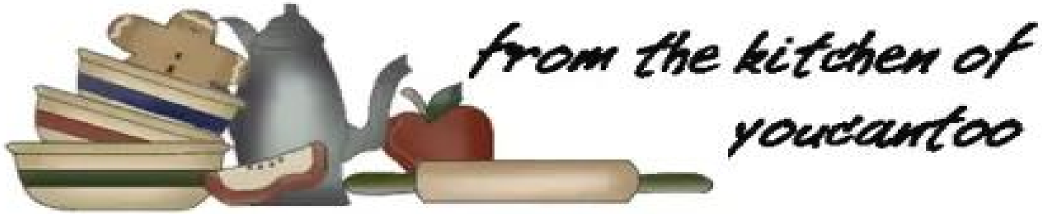
Undo the mounts and then reboot.

```
for i in /sys /proc /dev; do umount /mnt$i;
done
umount /mnt/boot/EFI # if necessary
umount /mnt reboot
```

Reboot again and that should do it.

Microsoft Windows has encountered an unrecoverable error. Please reboot and install PCLinuxOS.

PCLinuxOS Recipe Corner Bonus



Grandma's Old-Fashioned Bread Pudding with Vanilla Sauce

Serves: 12

INGREDIENTS:

8 cups cubed white bread
1 cup raisins
4 cups milk
1/2 cup butter
1 cup sugar

For the vanilla sauce:

1.5 cups milk
1.5 cups half-and-half
3 tsp vanilla extract
9 Tbsp sugar
12 large egg yolks.

DIRECTIONS:

Preheat the oven to 350°F (175°C).

In a large bowl, combine the cubed white bread and raisins.

In a saucepan, heat the milk and butter over medium heat until the butter is melted.

Pour the milk and butter mixture over the bread and raisins. Let it sit for 10 minutes to soak.

In a separate bowl, whisk together the sugar and eggs.

Pour the egg mixture over the soaked bread and mix well.

Transfer the mixture to a greased baking dish.

Bake in the preheated oven for 45 minutes, or until the top is golden brown and the pudding is set.

For the vanilla sauce:

Add the milk and half-and-half to a pot and bring to a simmer. Remove from the heat. Whisk egg yolks and sugar together in a bowl. Slowly ladle all the warm milk mixture into the egg yolk mixture while whisking quickly. Adding it too quickly will cook the egg yolks and cause the sauce to curdle.

Return the mixture to the pot and heat over medium-low while stirring until the sauce thickens and coats the back of the spoon, about 5 to 6 minutes. Remove from the heat and add the vanilla once it is no longer hot.

Strain the sauce if desired. Serve warm or chill in the refrigerator. To rewarm the sauce, add the sauce to a small pan and reheat it on the stove over low heat, while constantly stirring. Remove from heat once it's warmed through.

NUTRITION:

Calories: 693	Carbs: 107g	Sodium: 426mg
Fiber: 2g	Protein: 16g	

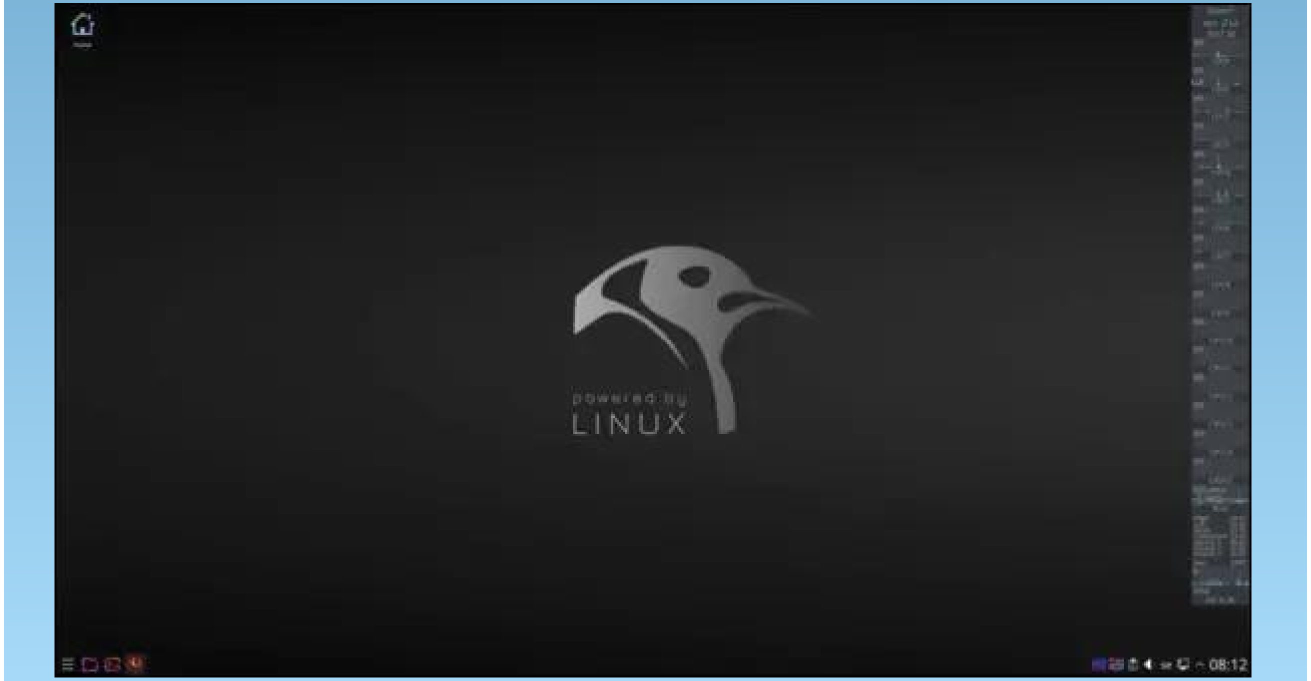
Donate To PCLinuxOS

Community Supported.
No Billionaires/Millionaires.
No Corporate Backing Or Funding.
Click here to make a one-time donation through Google Checkout.
Or, click one of the amounts down below to make a monthly, recurring donation.

Setup Error

Microsoft Windows has encountered an unrecoverable error. Please reboot and install PCLinuxOS.

Screenshot Showcase



Posted by scoundrel, on July 2, 2025, running KDE.

PCLinuxOS Puzzled Partitions

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

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

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

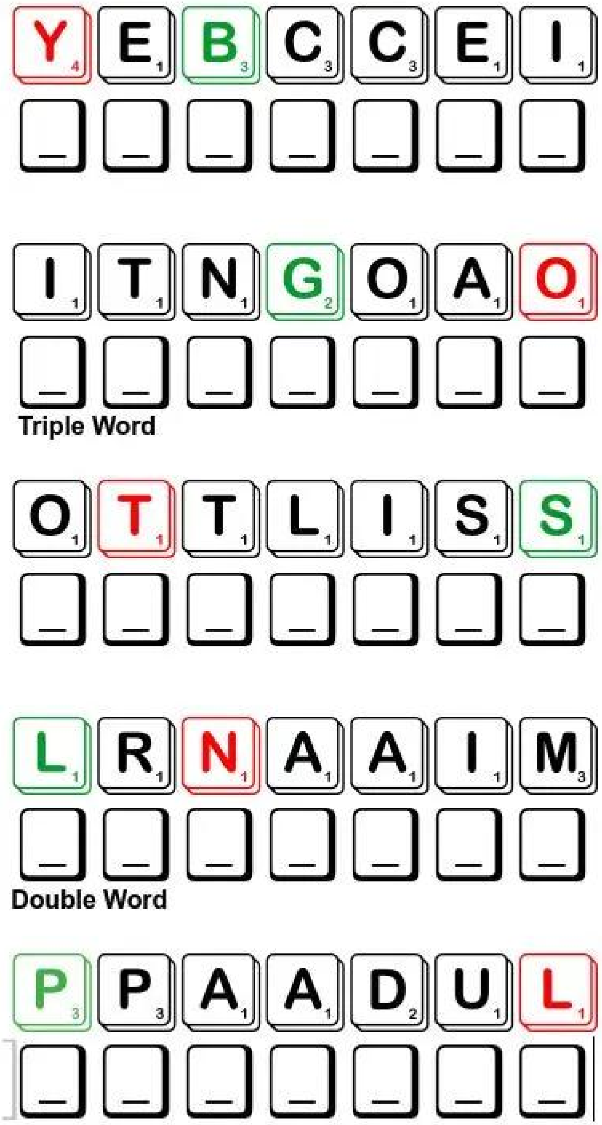
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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

SCRAPPLER RULES:

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

Download Puzzle Solutions Here



Possible score 210, average score 147.

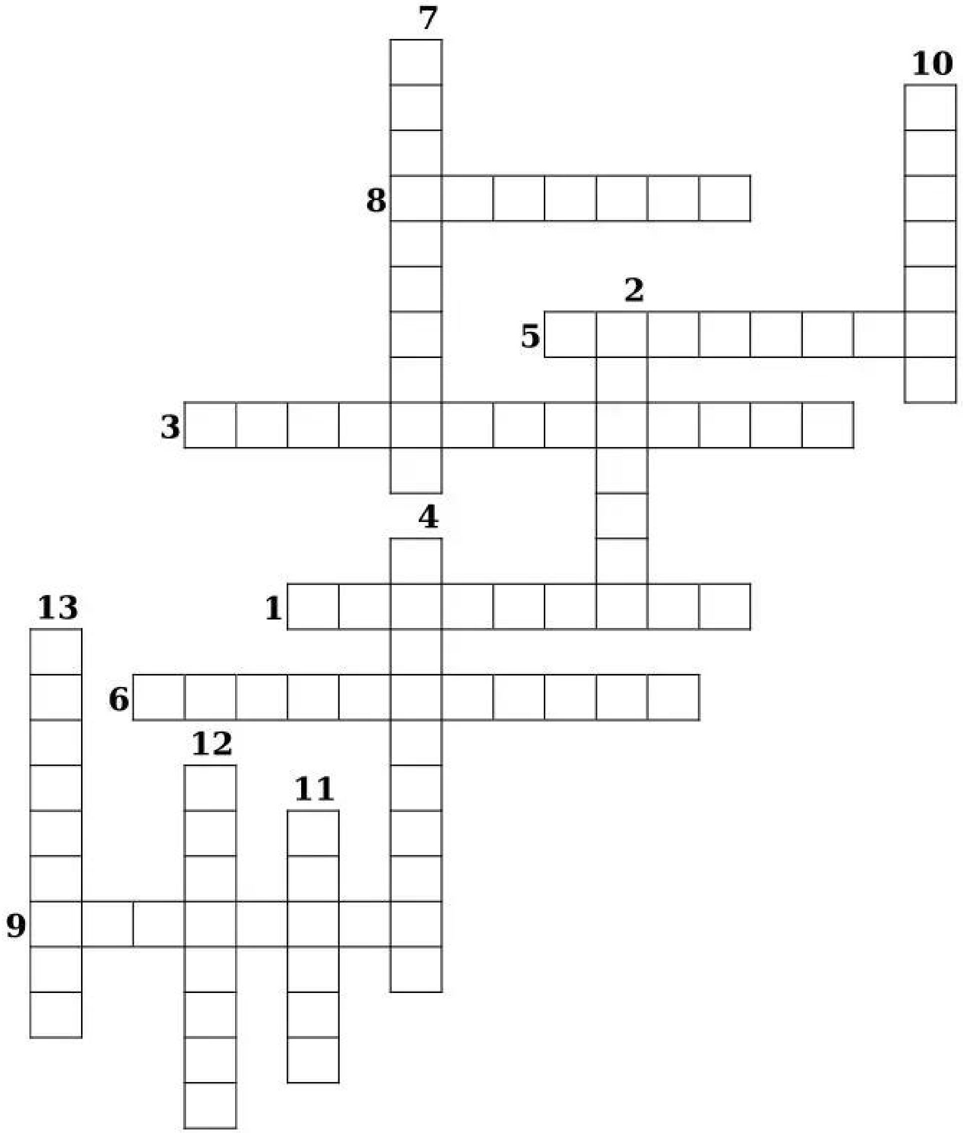
July 2025 Word Find
Going to the Circus

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

ACROBAT
ANIMALS
APPLAUD
AUDIENCE
BALANCING ACT
BALLOONS
BEAR
BICYCLE
BIG TOP
CALLIOPE
CANNON
COTTON CANDY
ELEPHANT
ENTERTAIN
FIRE EATER
GIANT
GRANDSTAND
GYMNAST
HORSES
HUMAN CANNONBALL
JUGGLER
KNIFE THROWER
LION TAMER
MAGICIAN
PERFORMER
POPCORN
RINGMASTER
SOMERSAULT
SPINNING PLATES
STILTS
STRONGMAN
SWORD SWALLOWER
TIGHTROPE WALKER
VANISHING ACT

Download Puzzle Solutions Here

July 2025 Crossword
Going to the Circus



1. The act of putting a flaming object into the mouth and extinguishing it as entertainment.
2. One who is skilled in feats of balance and agility in gymnastics.
3. One that performs exercises or stunts on a trapeze.
4. A roofed seating area at a stadium or arena.
5. A musical instrument fitted with steam whistles, played from a keyboard.
6. Melted sugar spun into thin threads and collected into a mass, usually on a stick.
7. A person in charge of introducing performers in a circus and guiding the audience through the show.
8. One who teaches or practices gymnastic exercises.
9. A person who performs tricks of illusion and sleight of hand for entertainment.
10. A person who tosses and catches objects like balls or knives, often for entertainment purposes.
11. A pair of long, slender poles each equipped with a raised footrest to enable the user to walk elevated above the ground.
12. A group of viewers or listeners of a work of art or entertainment.
13. A person who trains lions, especially for entertainment in a circus.

Download Puzzle Solutions Here

Mixed-Up-Meme Scrambler

BIGEE □ _ _ □ _

EAZUG _ _ □ _ □

ORPAND _ _ □ □ □ _

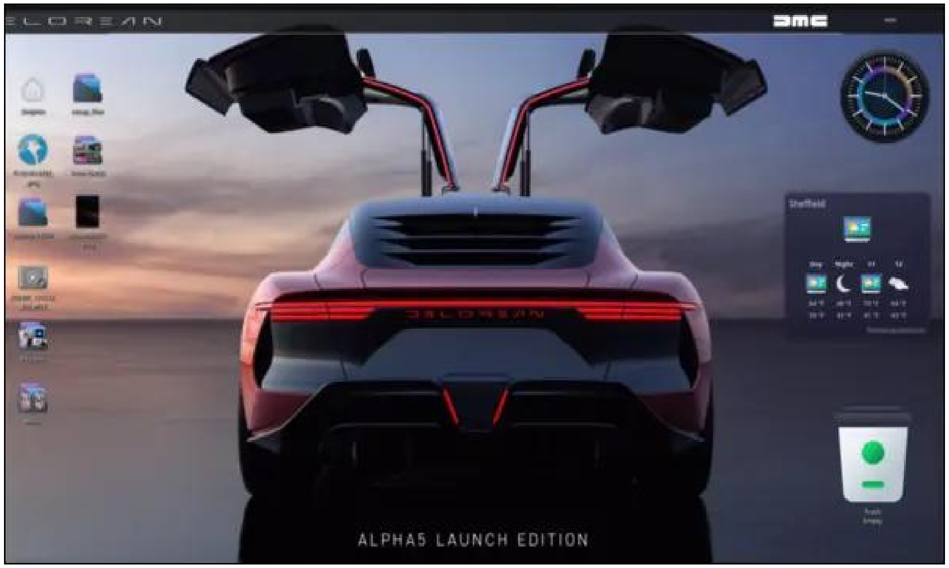
GOYAVE □ _ □ _ □ _

When the ants invaded their picnic, they ...

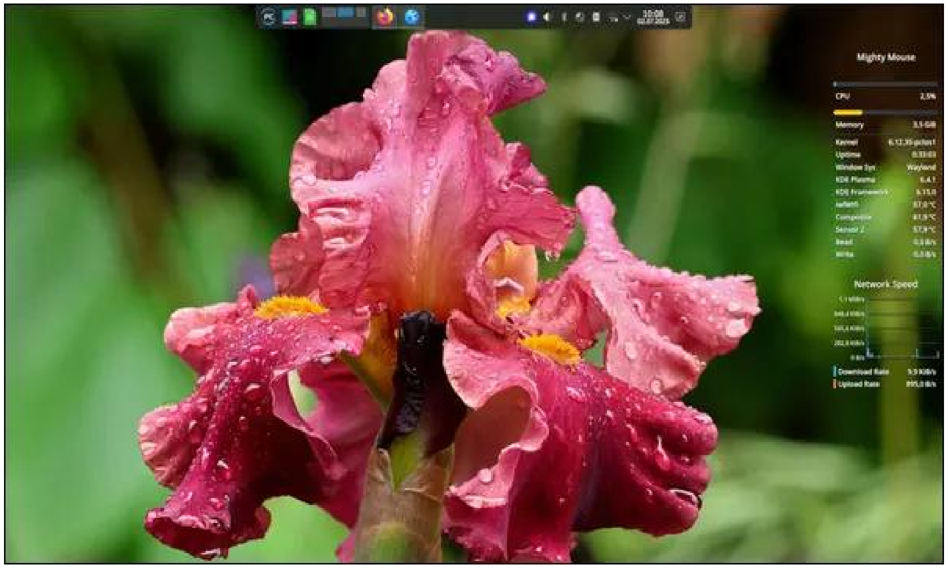
_ _ _ _ _ HER " _ _ _ _ _ "

Download Puzzle Solutions Here

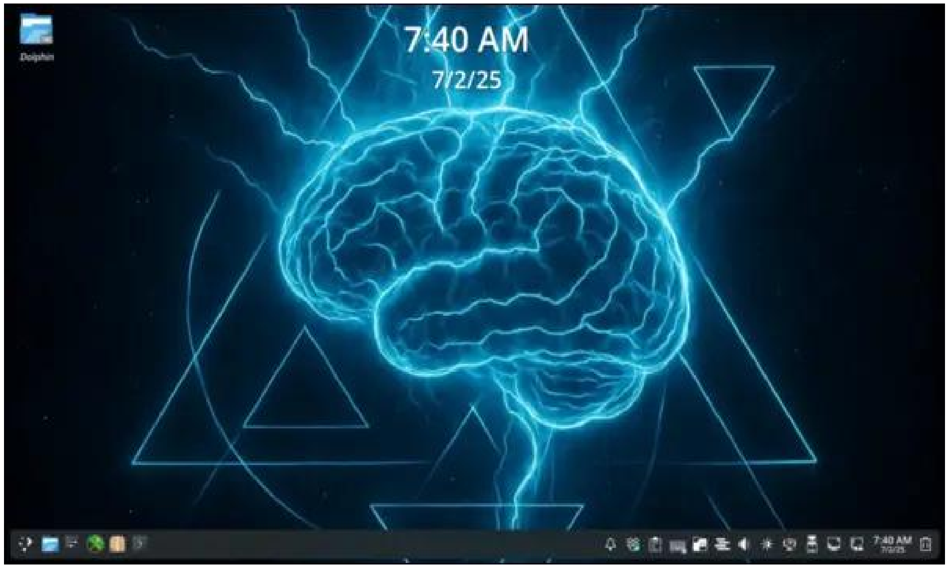
More Screenshot Showcase



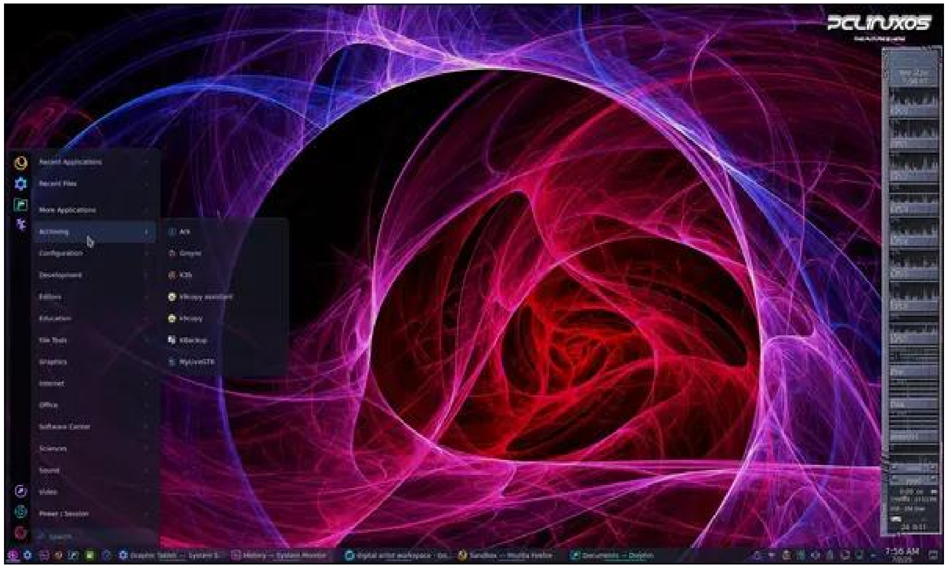
Posted by swarfendor437, on April 10, 2025, running PCLOSDebian KDE.



Posted by TBS, on July 2, 2025, running KDE.



Posted by Texstar, on July 2, 2025, running KDE.



Posted by Zoid, on July 2, 2025, running KDE.