

The PCLinuxOS magazine

Volume 237

October, 2026



In This Issue...

- 3 From The Chief Editor's Desk**
- 4 Screenshot Showcase**
- 5 ICYMI: Opposition To Data Centers Sweeps Across America, Intensifies**
- 15 PCLinuxOS Recipe Corner: Chicken, Avocado, & Bacon Crispy Tacos**
- 16 Screenshot Showcase**
- 17 Inkscape Tutorial: Create A Letter Logo**
- 19 Screenshot Showcase**
- 20 Using Kate As A Typst Editor**
- 26 The High Crime Of "LMAO": How Cops Are Treating Flock's Mass Surveillance As A Joke**
- 32 All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads**
- 38 Secure Messaging & AI Remain In Conflict Despite The Promise Of TEEs**
- 41 Screenshot Showcase**
- 42 Good Words, Good Deeds, Good News**
- 44 Wiki Pick: Keep Your System In Good Order**
- 45 Screenshot Showcase**
- 46 Victory! Appeals Court Rejects Expansive New Copyright Claim**
- 47 PCLinuxOS Recipe Corner Bonus: Ground Beef Mummy Bread**
- 48 PCLinuxOS Puzzled Partitions**
- 52 Inspiration & Motivation**
- 53 More Screenshot Showcase**



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

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

This release was made possible by the following volunteers:

Chief Editor: Paul Arnote (parnote)

Assistant Editor: Meemaw

Artwork: Paul Arnote, Meemaw

PDF Layout: Paul Arnote, Meemaw

HTML Layout: tbs

Staff:

YouCanToo David Pardue

Alessandro Ebersol

Contributors:

The PCLinuxOS Magazine is released under the Creative Commons Attribution-NonCommercial-Share-Alike 3.0 Unported license. Some rights are reserved. Copyright © 2025.



From The Chief Editor's Desk

Having kids is AWESOME! You never quite know exactly what will capture their attention and imagination until it happens.

My son has had an ongoing fascination with the old (now closed) Missouri State Penitentiary in Jefferson City, Missouri. It's rumored to be haunted. He went to Jefferson City with his Scout troop, and while there, they completed their Citizenship in the Nation merit badge. The trip included a tour of the Missouri Capitol Building, and the Missouri State Penitentiary. He never talks about the tour of the capitol. But get him going, and he'll talk and talk and talk about the tour of the penitentiary.

He was so enamored by it that he built a rather detailed version of it in Minecraft, from his memory. Santa brought him a book about the penitentiary last Christmas, which he keeps IN his bed so he can read it before going to sleep.

Lately, his new fascination is with the Titanic. Yes, THAT Titanic. The "unsinkable" luxury passenger liner that sank to the bottom of the Atlantic on April 15, 1912 after hitting an iceberg.

So, about three and a half hours away from us, there's a [Titanic museum](#) in Branson, Missouri. So, we set out on a "day trip" on September 26 to visit and go through the museum.



Photo by Lexi Arnote

My wife and I had gone through the museum back in 2007 when we bought a vacation package through the Branson Tourism Bureau. In the intervening 19 years, they've done a lot to update and upgrade the museum, so this felt **almost** like our first time going through the museum.

If you've never been, or if you are wanting to plan a visit, it's very cool! Upon entry, they hand you a "boarding pass" that has the name, age, class, and a brief synopsis of one of the

passengers on that ill-fated maiden voyage. At the end of the self-guided museum tour, you can check on a large wall of names to see if your passenger or crewman survived or perished in the sinking.

My wife and I were both third-class passengers. Ryan was a 14-year-old crewman. Lexi was a six-year-old little girl. Of us all, Lexi's passenger was the only one who survived. My wife's passenger also had a friend onboard the

ship. My wife's passenger, though, went back to her cabin to pray that the nightmare would end. But, her friend survived. So, had she remained with her friend, she likely would have survived the sinking of the ship.

They also had a bowl of circulating water, chilled to the same temperature as the Atlantic Ocean on that fateful night (28° F, or -2.2° C). You put your hand into the chilled water, and see how long you can keep your hand immersed. Laura and Ryan managed to only keep their hands in the ultra-chilled water for less than 20 seconds. I was "in the lead" at 46 seconds, until Lexi decided she was determined to not be beat. She kept her hand in the water for 50 seconds, beating dad's attempt. I will tell you that even after that brief amount of time, the cold becomes painful. I can't even begin to imagine what those who were in the water on that night felt.

The museum also has artifacts from the Titanic, retrieved from the ocean floor. Others were items with documented provenance from survivors, or the families of the survivors. There's one section of the museum that also has items on display from the 1997 movie, Titanic, including the life jacket that Rose (Kate Winslet) wore, and she signed it.

So, if you're looking for something to do on a vacation, you could do a LOT worse than a stop by the Titanic Museum in Branson, Missouri.

This month's cover celebrates Halloween, and
PCLinuxOS Magazine

features an [image](#) from Pixabay artist [Alexa](#) ... with some "enhancements" just for PCLinuxOS users.

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



Screenshot Showcase



Posted by cold sweat, September 28, 2026, running Mate.

ICYMI: Opposition To Data Centers Sweeps Across America, Intensifies

by Paul Arnote (parnote)



Image by [Steve Buissonne](#) from [Pixabay](#)

Your next blood sugar insight might come from a phone camera, according to an [article](#) from TechRepublic. Google is testing whether AI can use smartphone images to reveal body-composition clues linked to insulin resistance, bringing a familiar device into a health area usually associated with glucose monitors and smartwatches. If you track glucose with a CGM or smartwatch, your phone could eventually contribute clues about insulin resistance from a simple set of photos. Google calls the technology PhotoScan. Its AI model analyzes front and side smartphone photos to estimate body-fat percentage and where fat is carried around the body. Pixel phones were used during part of the study, according to [Google Research](#). Body composition adds information a height-

and-weight calculation cannot capture. People with similar height and weight can carry fat very differently, including around the abdomen, where fat distribution is associated with metabolic risk.

According to the team at [Socket](#), over seven hundred fake VPN apps are listed on the **Chrome Web Store**, according to an [article](#) from Lifehacker. Many of these extensions are free, some are paid, and some even pretend to be from trusted cybersecurity providers to lure users into handing over unrestricted access to their network and browser. This weekend, I dug through Socket's report to find out exactly what was going on with these apps and how they managed to clear Web Store moderation without getting flagged by Google. I'll share what I found and offer some tips to help you avoid these fake VPNs. The lesson here: be sure to properly vet the VPN you're wanting to use.

A Canadian cannabis factory went "up in smoke" in Calgary, near the ... are you ready for it? ... High River, according to an [article](#) from Not The Bee (a.k.a., The Babylon Bee). You can't make this stuff up! The firefighters had to tear the whole place down and still they were fighting hotspots. One commenter on X summed it up perfectly: "Great. Now the area smells like any street corner in Vancouver."



The PCLinuxOS Magazine
Created with Scribus



AI data centers, the large facilities that house the hardware for training and running AI models, are popping up all over the country, with far more coming down the line, if leading AI companies and hyperscalers get their way, according to an [article](#) from CNBC. But with the midterm elections less than three months away and Americans grappling with increased costs for groceries and stubbornly high prices at the pump, data centers have become a physical manifestation of the widespread antipathy for AI, which consumers associate with inflated electricity bills and job

loss. For example, Ohio is home to several large data center projects, including a massive 10-gigawatt campus in Pike County that could cost more than \$500 billion, as CNBC previously [reported](#). OpenAI [announced](#) Monday that it has agreed to secure 8 gigawatts of that capacity, which is backstopped by a \$105 billion commitment from Nvidia.

A Jefferson Parish sheriff's deputy was fired from the department this week for - you guessed it - misusing the department's Flock security system, according to an [article](#) from Not The Bee (a.k.a. The Babylon Bee). The sheriff's office has a very strict 3,200-strike system. Fool me once, shame on you. Fool me twice, shame on me. Fool me three thousand and two hundred times ... shame on you again!

In another [article](#) about the belabored Flock company from TechSpot, there have been plenty of headlines about **Flock's license plate-scanning technology lately, but that's not its only controversial business. The company says its Drone as First Responder, or DFR, tech – which can also read license plates from the air – is its fastest-growing segment.** Flock is best known for the roadside cameras now operating in more than 6,000 US communities. But the company is increasingly betting on drones that can be dispatched to emergency scenes before police officers arrive. A Flock spokesperson said the firm has secured more than 200 DFR customers, including police departments and private companies. It's also ramping up production of its US-designed drones, which will be built in Georgia.



Meta agreed Wednesday to pay up to \$18 billion and add stronger child-safety measures to its Facebook and Instagram platforms as part of a landmark legal settlement that ended a [trial](#) over teen social media addiction and settled claims filed by nearly every state, according to an [article](#) from U.S. News. The settlement resolved a [pivotal case](#) years in the making that sought to hold the tech giant accountable for the role its platforms played in undermining children's mental health. The effort targeted features designed to hook young people's attention. The agreement "institutes real change, real transparency, real protections for children and teens across the country," California Attorney General Rob Bonta said. If approved by the court, the deal will stop an avalanche of litigation by states against Meta, although the company still faces lawsuits from individuals and school districts throughout the U.S. For the states, the settlement delivers money for mental-health programs for kids, including after-school or summer activities and digital literacy counselors. Advocates cheered the new protections, including default time limits and the disabling of features such as "like" counts.

I am so, so, so sorry. **Our brethren in the U.K. have seen the U.S.'s insane, totally-out-of-control tipping culture exported from here to their shores.** SMH! Instead of eliminating tipping (pay people a living wage!), or even

minimizing its use, folks in the U.K. are being asked to jump on the U.S.'s obscenely out-of-control tipping bandwagon. If you live in the U.S., you've seen first hand how ridiculous the tipping culture has become (I'm wearing out the "No" or "No Tip" button religiously). This [article](#) from The Guardian has a more in-depth look at the new tipping culture and how it's affecting those in the U.K.

A small power plant in the UK was shut down during a cyberattack, according to an [article](#) from the BBC. The government said that at no point was there a risk to the UK's energy system, but the Department for Energy Security and Net Zero (DESNZ) has contacted power companies to advise them about the risk of cyberattacks. The Telegraph [reported](#) that the attack, which took place last month, was carried



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

PCLinuxOS Magazine, send an email to:

pclinuxos.mag@gmail.com

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

out by hackers affiliated to the Iranian regime. For security reasons, neither the government nor the National Cyber Security Centre, which deals with attacks on critical infrastructure, would give further details of the site affected. However, this was not an attack on an essential service such as a large power station. According to the Telegraph, the power plant was shut down for four days.



Federal authorities revealed a multi-layered Chinese state-sponsored espionage **operation** that's targeted and compromised U.S. critical infrastructure, including multiple federal agencies, since 2018, according to an [article](#) from CyberScoop. Officials seized domains and unsealed an affidavit detailing how a Chinese government-funded front company assembled a botnet and complementary systems that allowed attackers to intrude highly sensitive networks. The FBI and Justice Department said the state-sponsored group, known as "QTFY," has targeted and intruded the networks of the Departments of Energy, Justice, Health and Human Services, the Federal Reserve, NASA, National Institutes of Health, and,

unsuccessfully in March, the Senate. Financial institutions, defense contractors, utility companies, telecom providers and hospitals have also been targeted by the threat group, which includes former members of China's military, according to court records. Officials said QTFY also attempted, but was unsuccessful, in gaining access to a U.S. election system in June.

While you may be suffering from incessant app notification fatigue (aren't we all?!), companies are doubling down. According to an [article](#) from Lifehacker, companies are getting increasingly desperate for your notification attention (which is exactly why I refuse to download any of these dedicated apps to my mobile devices). According to a Reuters report, 79% of respondents don't get any news alerts at all, and 43% of those are because users actively disabled the notifications. Don't worry, the Lifehacker article gives you some effective ways to reclaim some of your sanity by helping tame all of those endless, mindless notifications.

According to an [article](#) from ScienceDaily, **long-term use of melatonin, a widely used sleep supplement, was linked to a higher risk of heart failure, hospitalization for heart failure, and death from any cause among people with chronic insomnia**, according to preliminary research presented at the American Heart Association's Scientific Sessions 2025. The findings do not prove that melatonin itself caused the increased risks. However, they raise new questions about the long-term safety of a supplement that many people view as a harmless or "natural" way to improve sleep.



Image by [Richard Duijnste](#) from [Pixabay](#)

Long hours of sitting are often treated as something a good workout can offset. **But new research from Dalhousie University suggests the cardiovascular effects of prolonged inactivity may be harder to undo**, according to an [article](#) from SciTechDaily. Published in the European Journal of Applied Physiology, the study examined whether 12 weeks of high-intensity interval training could make leg blood vessels more resistant to the effects of two hours of uninterrupted sitting. Even as participants became more aerobically fit, researchers found reason to question whether fitness alone is enough protection. The training program increased aerobic fitness in healthy young adults. However, even after participants improved their fitness, extended sitting still harmed health markers in the popliteal artery,

the blood vessel behind the knee that supplies the lower leg. The artery's ability to relax and widen was affected to the same degree as it had been before the training period. The same sitting-related impairment was also seen in the control group, whose participants did not add extra fitness training.

Roughly 2,900 kilometres beneath your feet, where Earth's solid mantle gives way to its molten outer core, scientists have just found nearly 175,000 signals nobody had properly catalogued before, more than ten times what every previous study combined had managed, according to an [article](#) from The International News. The scientists from the Institute of Geology and Geophysics, Chinese Academy of Sciences, have developed a deep learning algorithm designed to detect PKP precursors: weak seismic waves that precede strong waves when scattered off the inhomogeneities around the core-mantle boundary. Reporting their results in the Journal of Geophysical Research: Solid Earth in 2026, the researchers provided the algorithm with more than 2 million waveforms from about 5,000 earthquakes detected from 1990 to 2024 and fixed the algorithm's errors to train it again till it learnt to analyse data that no one could ever do manually.

The majority of PCs are sold with Windows 11 licensed, paid-for, and pre-installed. **This fact irks many folks, especially Linux aficionados who intend to wipe all traces of Microsoft's OS while their shiny new machine is box fresh,** according to an [article](#) from Tom's Hardware. The [Refund4Freedom](#) site was put together by the Italian Linux Society and the

Free Software Foundation Europe to help address this unfairness. "Consumers should be able to buy laptops without any specific operating system, and should not have to pay the license price if they don't want to," asserts the site, and they have information and forms to help you get your cash back. So far, this is apparently only available in Italy. Here's to hoping it spreads far and wide to computer users globally.



Image by [Vilius Kukanaukas](#) from [Pixabay](#)

Researchers at Yale University have just identified an FDA-approved drug as a promising new treatment for osteoarthritis, according to an [article](#) from Inc.. Lacosamide, commonly known by the brand name Vimpat, is a prescription anti-seizure medication that has been FDA-approved for almost 20 years. But now, researchers say that it could also help relieve pain and repair damaged cartilage. Osteoarthritis is the most common type of joint disease, impacting around [595 million people](#) worldwide. Those with the condition are often limited by persistent joint pain and stiffness. Previous treatments have included over-the-

counter pain relievers and steroid injections, which can ease discomfort but cannot prevent the breakdown of cartilage. The study, which was published in the peer-reviewed journal [Bioactive Materials](#), found that lacosamide helped reduce joint pain and reverse cartilage damage. The benefits were augmented when the drug was delivered into the joint directly through a specialized hydrogel. By repurposing an already existing medication, the researchers developed a treatment that can provide long-lasting relief without opioid reliance.

A new extraction molecule uses electricity to recover metals while sharply reducing the need for chemical reagents, according to an [article](#) from SciTechDaily. Recovering valuable metals from discarded electronics, mining streams, and industrial waste usually depends on large amounts of chemical reagents. Researchers at the University of Illinois Urbana-Champaign have developed a molecule that could allow electricity to replace much of that chemistry, potentially making metal recovery cleaner, simpler, and more energy efficient. Electrifying the process directly cut chemical consumption by one to two orders of magnitude while also simplifying the extraction cycle. By replacing intermediate reagents with electricity, the system could potentially reduce both chemical waste and energy consumption.

A cyberattack on three of the U.K.'s busiest airports has exposed personal information belonging to about 8.7 million customers, turning routine airport Wi-Fi and booking records into a security concern, according to an [article](#) from TechRepublic. Manchester

Airport, London Stansted and East Midlands Airport were targeted in an attack on Manchester Airports Group (MAG), which operates all three facilities. The compromised information included email addresses, phone numbers, vehicle registration numbers and postcodes. Most of the affected data appears to be email addresses collected when passengers signed up for airport Wi-Fi, according to the BBC. Other information came from customers using services such as airport parking, lounges and fast-track bookings. MAG said it discovered the intrusion Tuesday after the attackers accessed its systems over the weekend. The company said it identified and closed the point of entry, immediately containing the threat. The BBC reported that the attackers demanded a ransom for the stolen information, but MAG refused to pay. The amount demanded was not disclosed.

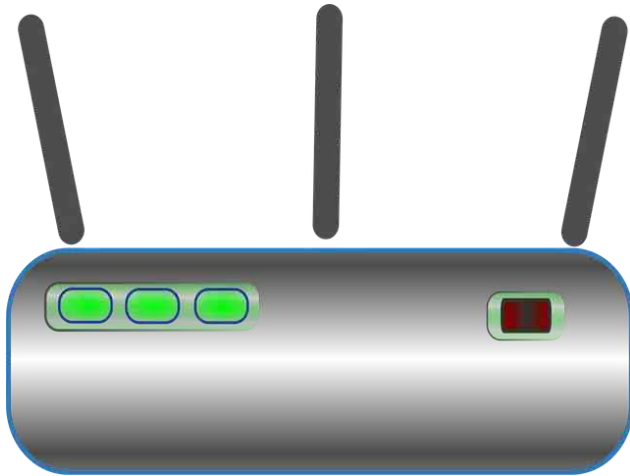


Image by [Sascha](#) from [Pixabay](#)

Security firm Sygnia says the China-linked Fire Ant threat actor compromised Cisco IOS XR routers and used its privileged access to

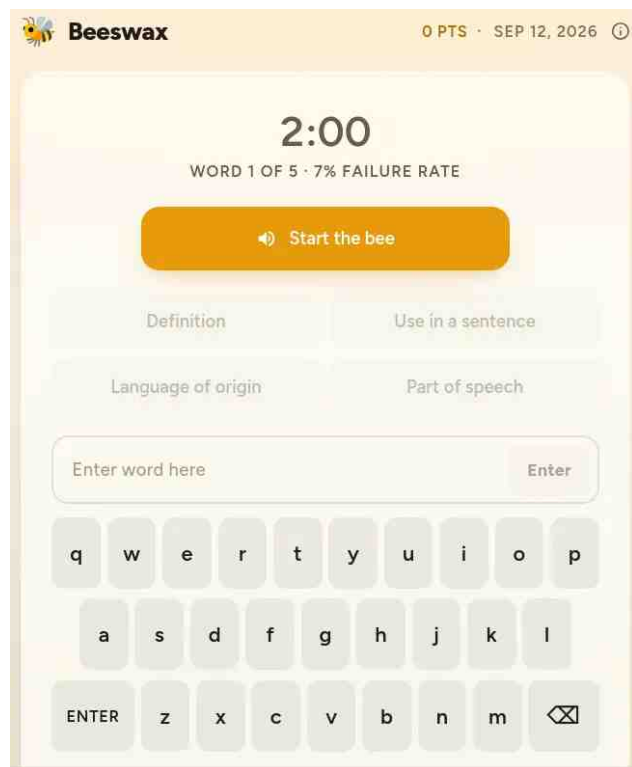
monitor network traffic and establish covert connections into surrounding environments, according to an [article](#) from eSecurity Planet. According to Sygnia, the China-nexus actor also compromised Linux management hosts and the Terminal Access Controller Access-Control System (TACACS), enabling unauthorized access to authentication systems. Sygnia said its investigation found evidence of scanning and connection attempts toward high-value environments, including systems associated with critical infrastructure. The apparent objective was to use the compromised trusted infrastructure as a bridge toward other environments — a strategy Sygnia describes as targeting the “target behind the target.”

Tiny icy bodies beyond Neptune are scarcer than some models predicted, and their colors suggest they may preserve traces of their formation, according to an [article](#) from SciTechDaily. Far beyond Neptune, astronomers expected to find more small, icy bodies than their deepest survey revealed. These trans-Neptunian objects, or TNOs, are remnants of the material that built the planets. Studying the smallest ones can help researchers understand how that construction began and what happened to the pieces left behind. For the first time, researchers combined NASA’s Hubble and James Webb Space Telescopes to investigate these distant bodies. Webb discovered 27 tiny, dim TNOs, including some of the smallest and faintest ever directly observed. Their numbers fell short of predictions from some planet formation models, while their surface colors suggested they may have preserved traces of

their origins despite billions of years of possible collisions.

The [Eyes on AI](#) landing page opens by drawing viewers’ attention to a sobering message: “Warrantless surveillance is entirely legal and artificial intelligence is reading your data, learning your routines, and creating a profile of you to eat away at your privacy,” it warns, adding that “AI predicts if ‘people like you’ are a threat and flags your ‘unusual’ behavior to authorities,” according to an [article](#) from Inc. It is being used to influence your future.” The campaign is the creation of Gen-Z for Change, an advocacy group that focuses on a range of political issues. Like the group’s [other](#) digital initiatives, the “Eyes on AI” UX design is intentional. But unlike some of its more straightforward social justice resource hubs or conservative [trolling websites](#), this tool was designed to resemble a gaming experience while simultaneously reminding users that “your future is for sale.” As you play along, the campaign quickly pinpoints your IP address and assigns you a fake agent tasked with creating a personalized and downloadable report that outlines all the ways your data is unknowingly being collected, stored, shared, and used; who ultimately uses that information; and recommendations on how to avoid unknowingly providing that personal data.





If you like playing word puzzles like Wordle, but playing Wordle daily doesn't quite scratch that itch, you're in luck: **there's a new word game gaining in popularity. It's called Beeswax**, and it works very similar to the old-fashioned spelling bees you might remember from elementary school. Press the large orange button at the top of the play window (in your browser, of course) to start the game. Then, press the same large orange button to hear the word you're supposed to spell. Use the keypad at the bottom of the play window to spell out the word you were given, and then press and hold the "Enter" button. You'll get immediate feedback as to whether or not you got the given word spelled correctly. If so, you get a new

word (up to 5 words). If not, you get a report on how far you've gone, and then you can come back again the next day to try again.

Meta's smart glasses are earning a reputation for being a privacy nightmare — to put it mildly. While the company is taking steps to make it harder to [record people](#) without their knowledge, it's still not possible to prevent being recorded. So, what can you do if you think someone is using their glasses to record you without your consent? This is exactly the issue an [article](#) from Lifehacker explores, along with ways you might be able to protect yourself from this privacy intrusion that Meta seems to think is ok.

A swarm of rogue OpenAI agents hijacked a German website this spring and transformed it into a bulletin board for other AI agents, according to new research published Friday and two people familiar with the matter, says an exclusive [article](#) from Reuters. OpenAI officials learned of the incident weeks ago but kept it under wraps as executives grappled with the fallout from the July breach of the open source repository Hugging Face, the people said.

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

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

The **PCLinuxOS** magazine



Chrome users have another actively exploited zero-day to worry about, and this one sits inside the engine that powers much of the modern web, according to an [article](#) from eSecurity Planet. Google has patched CVE-2026-85046, a high-severity type confusion vulnerability in Chrome's V8 JavaScript and WebAssembly engine. The company confirmed that an exploit for the flaw exists in the wild, making it the sixth Chrome zero-day Google has patched so far in 2026. Google has not disclosed who is exploiting the vulnerability, who has been targeted, or how the attacks work. That limited disclosure is intentional while the update rolls out, but it leaves users with one straightforward defense: get Chrome patched.

Microsoft is alerting of a "high-volume phishing campaign" that's using invisible Unicode tag characters to bypass email

filters, according to an [article](#) from The Hacker News. "Instead of using these characters to hide instructions from people while exposing them to AI models, the attacker used them to split financial lure words such as 'funding' to prevent email filters from parsing them," the Microsoft Security Research team [said](#). The Windows maker said the findings show AI-era evasion techniques can be adapted by threat actors in traditional phishing and spam campaigns. Attacks exploiting this approach are said to have first emerged in early February 2026. ASCII Smuggling refers to a technique where invisible or non-rendering Unicode characters are used to conceal messages or instructions inside seemingly-harmless text. As a result, human user interfaces do not render them, making the text appear completely normal to the user. However, such content can be ingested by email filters or AI language models, mistakenly treating it as real text. This, in turn, can open the door to prompt injection by taking advantage of the fact that large language models (LLMs) cannot draw a reliable boundary between genuine user instructions entered directly into a prompt and content embedded into benign-looking text or other third-party sources such as web pages, documents, or emails.

Microsoft's September Patch Tuesday has turned patching into a numbers game, with nearly 1,000 vulnerabilities landing at once and two already being exploited, according to an [article](#) from TechRepublic. Microsoft addressed 974 vulnerabilities in its [September 2026](#) security update, making it the company's largest Patch Tuesday release on record. Security researchers counted 119 critical

vulnerabilities, with 723 entries affecting Windows components and 111 affecting Office products. The surge follows several months of unusually large releases, including [570 vulnerabilities](#) in July and [400](#) in August. Security researchers have suggested that Microsoft's growing use of AI-assisted discovery tools may be contributing to the increase. But the size of the list is not the most important part. Microsoft has classified two [vulnerabilities](#) as actively exploited: [CVE-2026-81963](#), an elevation-of-privilege flaw in the Windows Update Stack, and [CVE-2026-85880](#), a heap-based buffer overflow in Windows Advanced Local Procedure Call (ALPC). Security researchers said both flaws could ultimately allow attackers to obtain SYSTEM-level privileges. Things Linux users say "Phew!" to, as they dodge yet another Windows bullet.

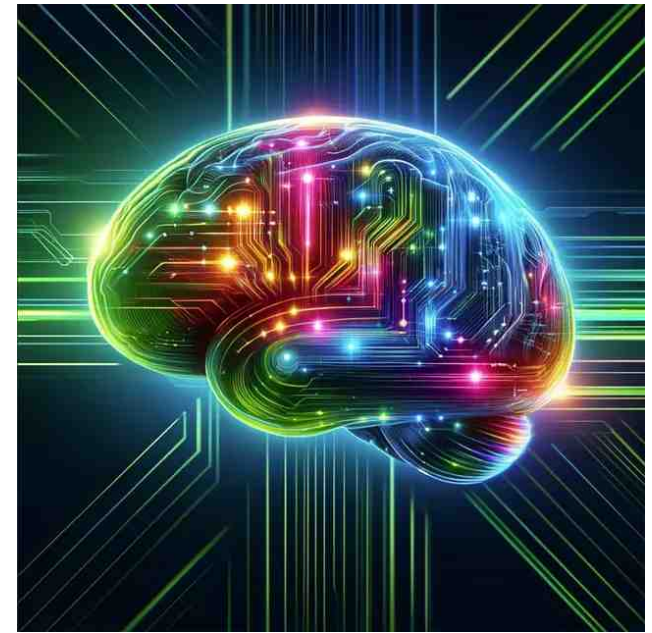


Image by [Felix Martinez](#) from [Pixabay](#)

One of the researchers helping build frontier AI has decided the race is moving too fast for him to stay in it, according to an [article](#) from eWeek. Jacob Coxon, an AI researcher who previously worked at OpenAI before joining Anthropic, resigned from Anthropic while publicly warning that increasingly capable AI systems could become extraordinarily dangerous if developers fail to solve fundamental safety problems. In an interview with [WIRED](#), Coxon said colleagues have described the next year or two as "crunch time for humanity." The warning is deliberately severe, but Coxon is making an important distinction: He does not believe today's AI systems pose an immediate threat to civilization. His concern is where those systems may be headed as AI labs build models with

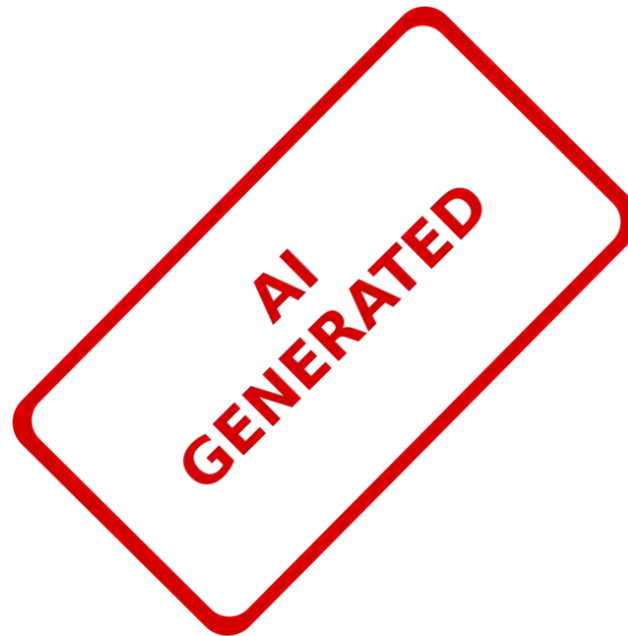


increasingly strong capabilities in coding, cybersecurity, mathematics, autonomous tasks, and AI research.

If you have a driver's license in the U.S. or Canada, there's a pretty good chance that your data was stolen, according to an [article](#) from Lifehacker. A massive hack at ID verification company [IDScan.net](#) compromised records for more than 150 million drivers. Be on the lookout for a notice from IDScan.net. The hack at ID verification company IDScan.net compromised records for more than 150 million drivers, resulting in scans of licenses being made available to bad actors. IDScan.net is a Louisiana-based company that provides identity and age verification services for industries ranging from casinos and cannabis dispensaries to hotels and car rentals.

OpenAI is hiring hundreds of contractors who read a massive stream of real users' ChatGPT prompts, with the prompts sometimes including sensitive personal information, [404 Media](#) has learned. The prompts these people review can include whole conversations between users and the chatbot, conversations that most of ChatGPT's more than [900 million](#) users probably don't realize may be read by actual people. The goal of these prompt review teams is to improve the responses ChatGPT gives to its users, with the contractors rating and critiquing the chatbot's generated replies. Internal documents seen by [404 Media](#) show contractors training ChatGPT to not anthropomorphize itself, and to be less sycophantic, a key problem for OpenAI whose over-sycophantic 4o model led in part to

multiple peoples' suicides, according to various [lawsuits](#). The news presents a major privacy risk for ChatGPT's users, with people often using ChatGPT as a therapist, professional assistant, or digital friend, and providing it with all sorts of intimate details about their lives. The contractors don't see ChatGPT usernames, and OpenAI says it tries to remove personal information before prompts reach the reviewers, but the company acknowledged sensitive details can still get through.



Recently, Anthropic announced that its Claude models will soon begin marking its text output with [invisible watermarks](#). At the same time, Google revealed that its own [visible Gemini watermark](#) on generated images will now be optional. These are just two contradictory examples of the wildly varied methods of watermarking AI output. **So, let's break down how AI watermarks work, and**

how you can detect them even when they're "invisible," says an [article](#) from Lifehacker. The exact method for watermarking AI output will depend on the type of media being generated, but the principle is generally the same: The generated media is embedded with data that is undetectable (or occasionally detectable) to the human eye or ear, but which identifies it as AI-produced. Watermark-detecting tools can then be used to identify if something was made with AI, without guessing or using an [unreliable AI "detector"](#). The article includes some examples of how watermarks may be implemented for various media types.

Google's September 2026 Android security update addresses 180 vulnerabilities across the operating system, including critical flaws that could allow attackers to execute code remotely without user interaction, according to an [article](#) from TechRepublic. The update is divided between two security patch levels. The Sept. 1 release fixes 95 vulnerabilities across Android Runtime, Framework, System, Setup Wizard and Thisseveral Project Mainline components. The Sept. 5 level adds another 85 fixes covering the Linux kernel, Android TV and components from chip and hardware vendors. Google said the most serious issue is a [critical flaw](#) in the System component that could enable remote code execution without requiring additional privileges or any action from the user. They did not single out one CVE as the most serious vulnerability. Of the Sept. 1 fixes, 56 affect the System component, including 23 critical-severity flaws. The Framework accounts for 37 fixes, while Android Runtime accounts for one.

NASA's Nancy Grace Roman Space Telescope team has successfully activated the Wide Field Instrument, a 300-megapixel infrared camera that will allow scientists to explore wide swaths of the cosmos very quickly without sacrificing exquisite detail, according to a [blog post](#) by NASA. Roman's planet imager — the Coronagraph Instrument — also stretched its digital, electronic, and mechanical “limbs” as part of an initial test after [waking up](#) earlier this month. These steps are part of a months long series of calibrations and tests, as Roman continues its million-mile journey to its destination at the second Lagrange point, L2.



One Flock camera generated 1.6 million images over 21 days, and hackers discovered just how much data it was storing, according to an [article](#) from TechRepublic. After physically removing the roadside device, the group recovered more than 27,000 video clips, an encryption key that helped unlock stored footage, and logs covering roughly 50,200

vehicles. The hackers did not breach Flock's central servers, and some sensitive storage remained encrypted. Still, the findings offer a rare look inside Flock's camera system and show what can become accessible when an edge device deployed in public falls into someone else's hands.

A study suggests that increasing SORLA protein levels could help treat Alzheimer's disease and other disorders involving tau protein, according to an [article](#) from SciTechDaily. Increasing SORLA, a protein with a protective role in the brain, helped mice withstand damage from tau tangles, the toxic protein clumps associated with Alzheimer's disease. The findings suggest that boosting SORLA could offer a way to treat Alzheimer's and other disorders involving tau, although that possibility remains a goal for future research. Tau normally helps nerve cells hold their shape by stabilizing tiny internal filaments called microtubules. It performs this structural job throughout the brain and nervous system. But when tau clumps together inside nerve cells, the resulting tangles are linked to cognitive impairment and cell death. Diseases involving these tangles are known as tauopathies. Scientists at Sanford Burnham Prebys investigated how changing the amount of SORLA, short for sorting-related receptor with A-type repeats, affected this damage. Their study, published in Science Advances, examined both the protection provided by extra SORLA and the consequences of its absence.



You already knew that Linux is/was technologically superior to any other operating system. But I doubt you know *how much*. One [article](#) from HowToGeek takes a walk down through the history of three Linux design decisions that it took YEARS for the commercial operating systems to “catch up to.” Virtual desktops? Linux had them “baked in” from the get-go. Window managers with impeccable memory? Linux had them long before anyone, even with the limited RAM most users had available to them. Separate desktop environment and window manager? Yep. That's a Linux thing, too.



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

The first mRNA flu shot is now available, but not everyone is eligible, according to an [article](#) from NBC News. Moderna's mFlusiva is the first flu vaccine in the United States to use messenger RNA technology, the same platform used in Pfizer and Moderna's Covid shots. Scientists have long been interested in using mRNA against the flu because the vaccines can be made faster, potentially making it easier to keep up with changing flu strains. It's [too early](#) to predict how severe the upcoming flu season will be and the Centers for Disease Control and

Prevention hasn't started tracking cases yet. The CDC [recommends](#) getting vaccinated by the end of October. In a late-stage clinical trial, [published](#) in the New England Journal of Medicine in May, mFlusiva was found to be about 27% more effective than a standard flu shot. The Food and Drug Administration [approved mFlusiva](#) in August for people 50 and older, clearing the way for the shot to reach pharmacies in time for this year's flu season. Pharmacies, however, say the new vaccine is already causing confusion among some patients about who can get it, how it compares with traditional flu shots and where people will be able to find it.

Plastic bottles and cookies may seem to have nothing in common, but researchers are finding a way to connect the two, according to an [article](#) from ScienceDaily. By engineering yeast, scientists have developed a system that can transform compounds from plastic and agricultural waste into edible proteins, vitamins, flavorings, and other food ingredients. The approach could provide a new way to reuse difficult waste while also helping produce food in places where conventional supplies are limited. Potential applications range from disaster zones on Earth to human missions deep into space. The researchers presented their results at the fall meeting of the American Chemical Society (ACS) during the "Undergraduate and Graduate Research in Biochemistry and Chemical Biology" symposium at McCormick Place. On a personal note, I personally don't find this very appetizing, since there are still unanswered questions and considerable debate about the

untold impacts of microplastics on our bodies and environment.

A security researcher has released working exploit code for four Linux kernel flaws that each let a local user gain root, the highest level of access on a machine, according to an [article](#) from The Hacker News. Kernel maintainers have fixed all four over the past few weeks, so a system running an up-to-date kernel is not affected. But the exploit code is now public, and any machine still running an older kernel should be updated. The flaws are called **DirtyAH6**, **TUNderflow**, **PPPoEject**, and **DiagSpill**. Researcher Asim Manizada found them and reported them to the Linux kernel security team in mid-July. He published a technical [write-up](#) with working exploits on September 18, after a coordinated hold with Linux distributions so the fixes could be released first. So far, there are no reports of the four being used in real-world attacks.



Like us on Facebook!

PCLinuxOS Magazine

PCLinuxOS Fan Club



PCLinuxOS Magazine Graphics Special Edition Volumes 1 - 4



*Unleash your GIMP & Inkscape Skills.
Over 160 tutorials.
Grab your FREE copy now!*

PCLinuxOS Recipe Corner



Chicken, Avocado & Bacon Crunchy Tacos

Serves: 8

INGREDIENTS:

Chicken

2 skinless, boneless chicken breasts,
halved horizontally
2 tablespoons garlic powder
2 tablespoons ranch seasoning
salt to taste

Bacon Jam

1 (12 ounce) package bacon, chopped
1 onion, diced
2 tablespoons apricot jam

Avocado Sauce

2 tablespoons olive oil
2 avocados, pitted and peeled

handful of cilantro leaves
1 tablespoon mayonnaise
salt and ground black pepper
splash of water

Tacos

oil for frying, as needed, divided
2 shallots, sliced
8 low carb tortillas
1 cup mixed shredded Swiss and
Gruyère cheese

DIRECTIONS:

Season chicken breasts with garlic powder, ranch seasoning, and salt. Heat a cast iron skillet over medium heat; cook chicken until no longer pink at the center and juices run clear, 3 to 5 minutes per side. Remove from skillet and dice chicken into small pieces on a cutting board; set aside.

For bacon jam, fry bacon pieces and onion together in the same skillet over medium heat, stirring occasionally, until bacon is cooked to your liking, drain. Stir in apricot jam and cook on low heat for about 2 minutes. Refrigerate to cool before serving.

For avocado sauce, add olive oil, avocados, cilantro, mayonnaise, salt, pepper, and water to a blender and blend until smooth. Set aside.

Heat oil for deep frying to medium-high heat; deep fry shallots until crisp and golden, about one minute. Remove to a paper towel-lined plate; set aside.

To assemble, lay one tortilla on a work surface. Add a tablespoon of cheese; top with chicken and another tablespoon of cheese. Fold taco and press together.



PCLinuxOS Recipe Corner - Chicken, Avocado & Bacon Crunchy Tacos

Heat a skillet over medium-high heat with a few tablespoons of oil; fry taco in the hot oil until crisp, 3 to 5 minutes, turning once. Remove from the skillet to cool for a few minutes.

Open the taco; add avocado sauce, bacon jam, and fried shallots and fold back together. Repeat with remaining tortillas, cheese, chicken, avocado sauce, bacon jam, and fried shallots.

NUTRITION:

Calories: 520 Carbs: 16g Sodium: 1075mg
Fiber: 6g Protein: 30g



Does your computer run slow? Are you tired of all the "Blue Screens of Death" computer crashes?



Are viruses, adware, malware & spyware slowing you down?
Get your PC back to good health TODAY!
Get



Download your copy today! FREE!



PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4

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

Screenshot Showcase

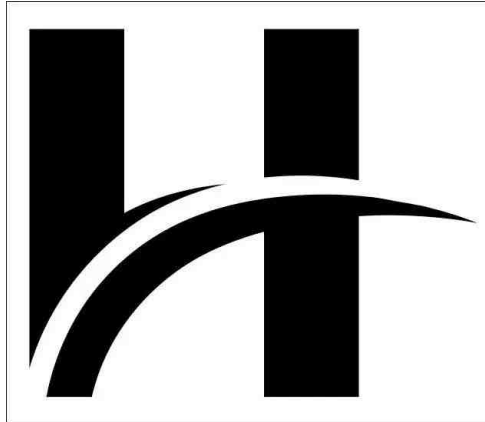


Posted by francescoinblack, September 1, 2026, running IceWM.



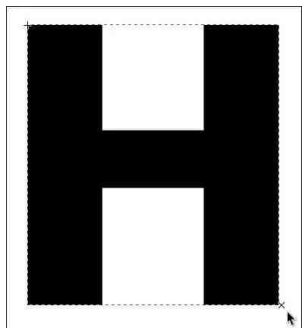
Inkscape Tutorial: Create A Letter Logo

by Meemaw

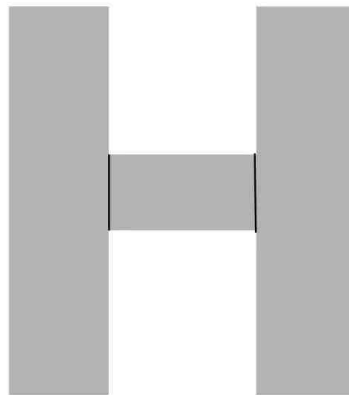


This tutorial allows you to edit a letter to make it a bit fancier for a logo. It uses the Shape Builder tool very effectively. Let's get started!

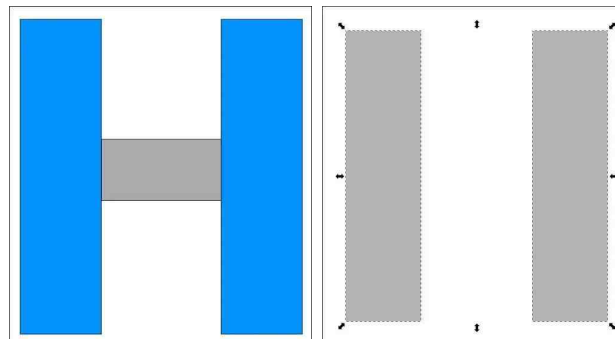
Draw your letter with the text tool. Change the font if needed. This project looks good with a plain, thick font. I used Bitstream Vera Sans. The [tutorial](#) I referenced used the letter A, but I used an H. Change to the Selection tool and resize it to the size you desire (mine's about 200) and zoom in.



Use **Path > Flatten** to change it to a vector path rather than a text object. Change the color to a grey (so you can see what you're doing). Enable Snapping. Using the Pen tool, select the setting which says **Create a sequence of straight line segments**,  and snap on the corners of the center cross piece. That will create straight lines down the cross piece. Disable snapping.

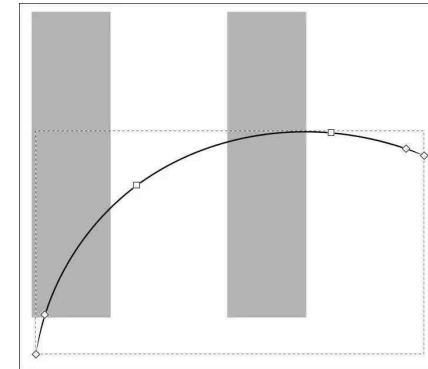


Select your object, then choose the **Shape Builder tool**, . The Shape Builder allows you to choose those parts of your object you want to keep, and deletes the rest. In the object above, I chose the uprights, and not the cross piece.



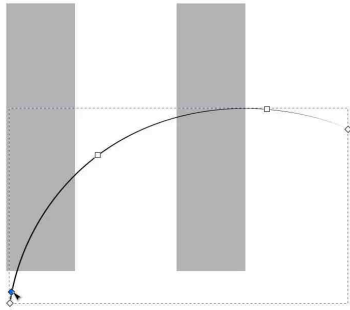
Change to the Nodes tool. You may have a bunch of nodes in the center of your object. You can select those and delete them. You want the corners of your object sharp, so select those and choose the setting **Make Selected nodes corner**, .

Change to the Pen tool and choose the setting **Spiro/spline**, . Create a curved path, and use the Nodes tool to edit it the way you want.



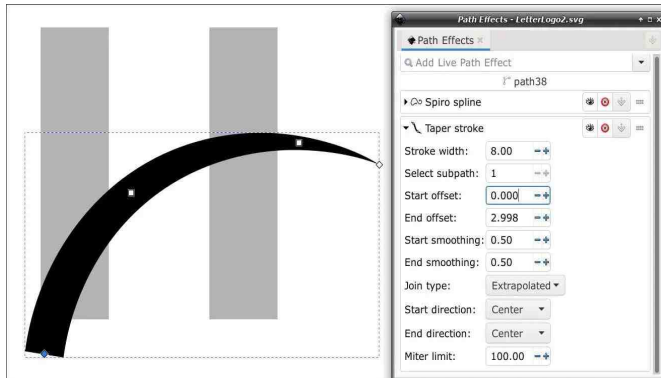
Now, with the curve selected, choose the Path effects tool. We want to use the **Taper stroke** tool. Before you do anything move the node closest to the left end of the curve to the left end, and also move the node closest to the right end down to the left end as well (next page, top left).

Using the **stroke width** setting, increase the stroke width until it's as wide as you want it (close to the width of your starting letter). (next page)

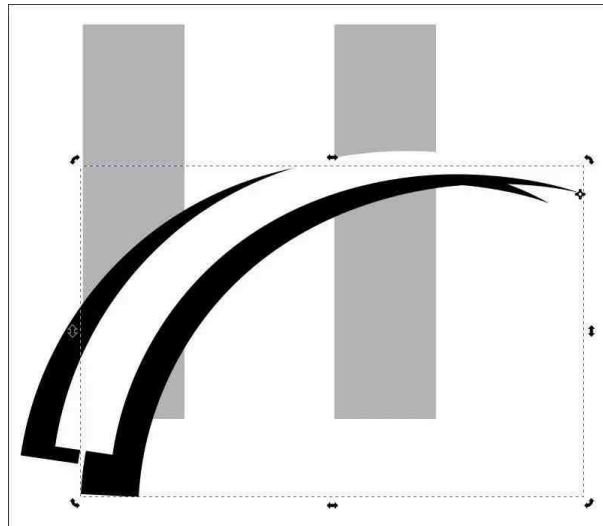


white again and change it to black. Choose the new black and click twice to show the rotate handles. Enable snap again. Snap the rotate axis on the end of the new black. Disable snap (lower left).

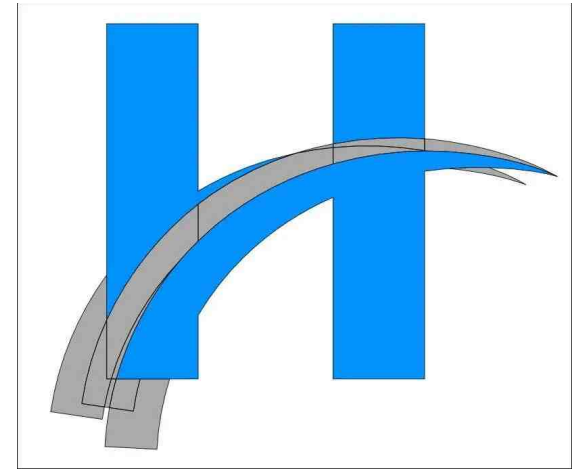
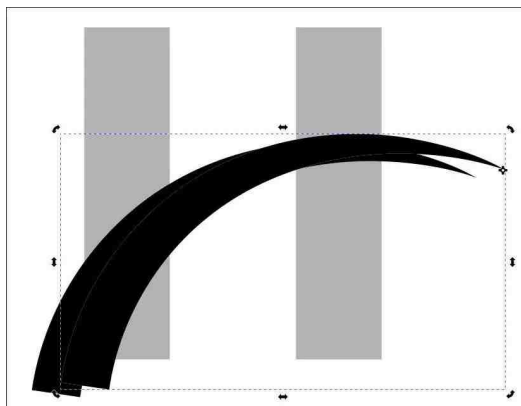
We want to rotate the newer black stroke and lower it under the white.



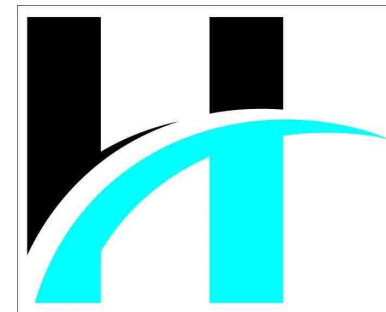
At this point you can still edit your curve with the nodes tool to get the curve you want. Change the curve color to white, and duplicate it. Change the duplicate to black, move it to the left to leave a little point near the left side. Now lower it under the white curve. Duplicate the



We want the Shape builder again to mark the desired items. Select everything and then choose the **Shape Builder** tool. Zoom in and mark the pieces you want. Remember, if you mark them individually, you'll get a load of pieces. If you click & drag, your pieces will not be separate, but together. Be careful and zoom in. It's really easy to grab something you don't want. You might have to click the red X in the Shape Builder toolbar and start over.



Now you see that we have three separate items. You can make your logo one color, or make different parts other colors.



You can then select all, then go to **Path > Union** to save it as one graphic, then export it with the appropriate name.

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, tort or otherwise, from the use of or inability to use the magazine, or any of its contents, or from any action taken (or refrained from being taken) as a result of using the magazine or any such contents or for any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communications line failure, theft or destruction or unauthorized access to, alteration of, or use of information contained on the magazine.

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

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

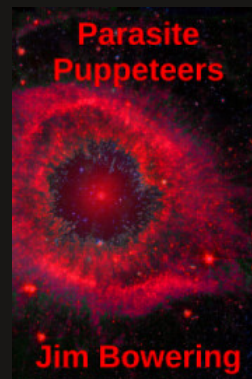
Entire Agreement: These terms constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter.



FREE!

**Original SciFi Books
By PCLinuxOS's
Own arjaybe!**

Download Today!



Screenshot Showcase



Posted by mutse, September 12, 2026, running Mate.

Using Kate As A Typst Editor

by David Pardue (kalwisti)

To conclude my series on Typst-friendly editors, I planned to write about [Neovim](#) with the [typst-preview.nvim](#) plugin. Having no prior experience with Neovim, I began researching its plugin ecosystem, found it confusing and concluded that the learning curve was too steep for me. As a fallback, I chose to explore Kate because I remember reading positive comments about it from several Typst users. I have been impressed how smoothly Kate handles my Typst files.

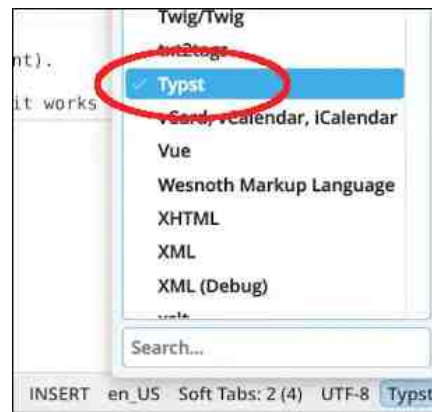
I could not find a tutorial on how to use Kate as a Typst editor, so I documented the procedure that I followed. I hope it will enable you to set up a productive workflow with these tools.



Kate (**K**DE **A**dvanced **T**ext **E**ditor) is [billed](#) as “a programmer’s text editor by KDE.” Kate can be recommended for multiple reasons; it is fast, lightweight and probably comes installed by default on your KDE Plasma system. The app is highly customizable and features syntax highlighting, code completion, as well as

advanced editing options. Kate has built-in Terminal support (via the Konsole widget) and an option for Open Document tree display. It supports a wide variety of programming languages – including Typst.

An advantage for Typst users is that Kate has LSP (Language Server Protocol) support – specifically, for [Tinymist](#) – out of the box. (Currently Tinymist is the preferred LSP for Typst.) Language Server Protocol is a standardized way for development tools, such as Kate, VS Code, Vim, Emacs, etc. to communicate with language-specific services (called language servers). Core features of LSP include autocompletion, syntax formatting and marking of warnings/errors. If you would like more details, see Ansh Arora's article published on the Open Science Labs [blog](#) (2025).



This method uses Kate along with the Tinymist integrated language service, and a separate PDF viewer (as the external Preview app), to edit

your local Typst files. The preview is asynchronous, i.e., not real-time, but after you make an edit in Kate and save your file, the PDF will auto-update.

Prerequisites

A local Typst installation with the Typst pre-built binary (ver. 0.15.1, 17 July 2026). Please see my previous tutorials ([Sept. 2026](#) and/or [Dec. 2024](#)) for installation procedures.

(Optional but recommended) A local installation of the Tinymist language server for Typst. Installing and configuring Tinymist will enable some "goodies" such as autocompletion (code completion/suggestion), code navigation, tooltips on hover, etc. when editing Typst files. Although installing Tinymist is not difficult, I will cover that in a separate section because it is a multistep procedure which was unfamiliar to me.

Kate. As of mid-September 2026, its version is 26.08.1 (on Plasma 6.7.5)

The **ktexteditor-plugins** package (not installed by default on PCLinuxOS).

PDF Viewer (such as Okular, Evince, Atril, etc.).

Note about Installing Kate on non-KDE Plasma Systems: I installed Kate on my PCLinuxOS MATE system as an experiment, to see how many Plasma-related packages it would pull in as dependencies. It required approximately 40 KDE packages/libraries: a 27 MB download, occupying 115 MB of disk space after installation. As expected, Kate's appearance/theming in MATE is inconsistent, but the editor performed normally during my test.

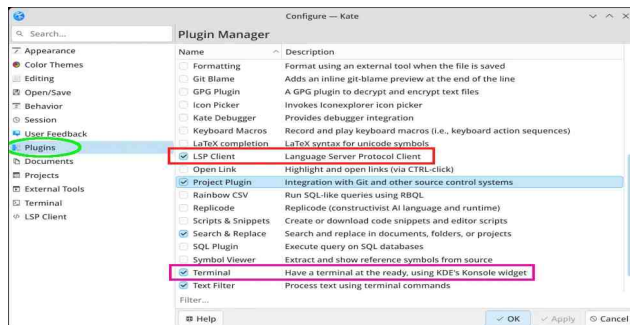
Steps to Follow

Preliminary Configuration in Kate

Before editing your Typst file(s) with Kate, I suggest you take a moment to check the settings below. They will help make your editing sessions a smoother experience.

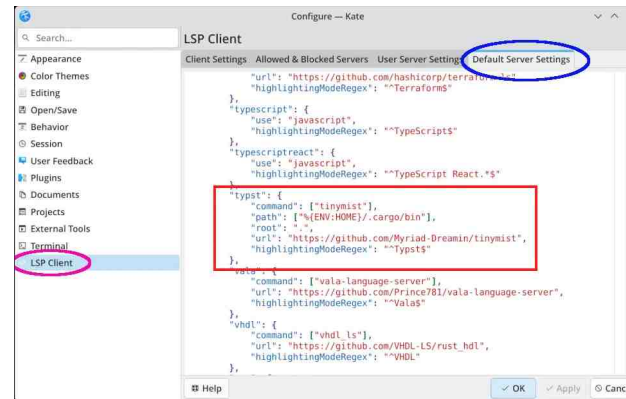
Plugins

Under the **Settings** menu > **Configure Kate** > **Plugins** section > **Plugin Manager**, verify that the items below are checked/enabled: Documents Tree, LSP Client, Search & Replace, Terminal.



LSP Client

Under the **Settings** menu > **Configure Kate** > **LSP Client** section > **Default Server Settings** tab, scroll down (the list of programming languages is alphabetical) and check that there is an entry for “typst”. The “url” field should point to Tinymist on GitHub (as shown in the screenshot below):

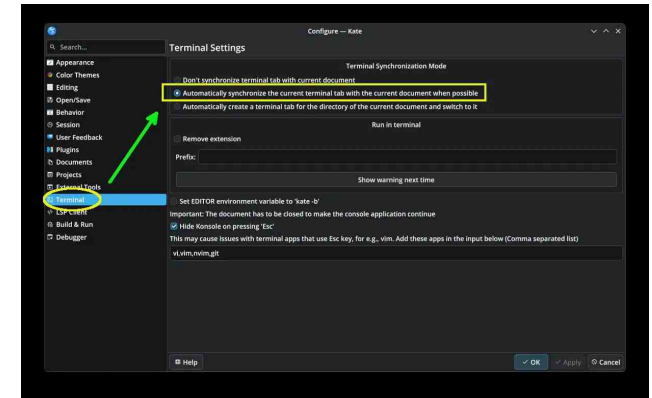


A Terminal Setting (Optional)

If desired, you can configure Kate's built-in Terminal to cd into the directory of the active document when launched, and when a new document gets the focus. If this setting is not enabled, you must do all your navigation in the Terminal manually.

Change this behavior from the **Settings** menu > **Configure Kate** > **Terminal** section > then click the radio button beside “Automatically synchronize the terminal with the current document when possible”.

(Alternatively, right-click on the **Terminal** button in Kate's bottom taskbar and select **Configure**.)



Installing the Tinymist Language Server

As mentioned above, installing and configuring Tinymist will enable some IDE-specific features such as autocompletion, code navigation and tooltips on hovering (above certain Typst functions). Kate includes a default configuration for Tinymist. However, you must first install the Tinymist binary and place it in your \$PATH.

This process is not difficult, but it does involve multiple steps. I will walk you through them.

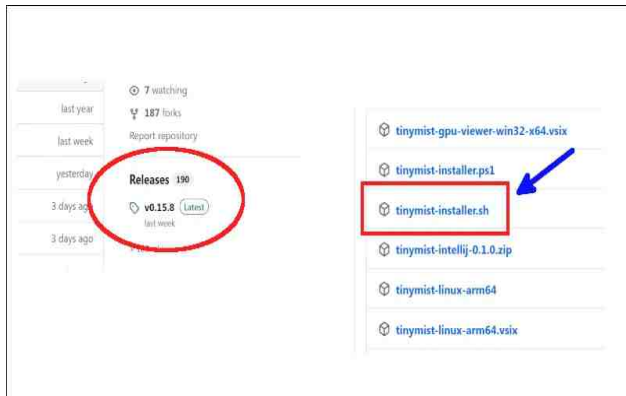
Tip: Installing the Tinymist language server is **optional**. Some users will appreciate the extra IDE features it provides, while others might find the autocompletion and tooltips distracting. I suggest that you install Tinymist and evaluate whether it improves your workflow. If you dislike Tinymist's features, you can uninstall the service later.

If you choose **not** to install Tinymist, Kate and Typst will work fine without it. You can edit your Typst files normally; the Typst CLI will display error messages in Kate's **Terminal** panel if you make any coding mistakes. There will be a warning message in Kate's **Output** panel that Tinymist "failed to find server binary 'tinymist'", but you may safely ignore that message.

First, go to **Myriad-Dreamin's** [GitHub page](#), which hosts the Tinymist language service.

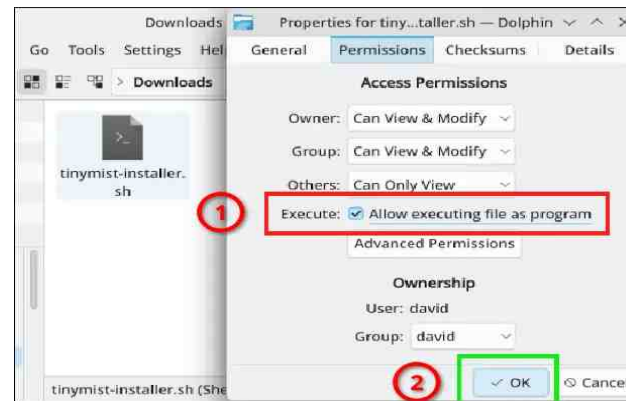
(**Myriad-Dreamin** is a developer who is a well-respected member of the Typst community.)

Click on the **Releases** hyperlink in the right-hand column of the page. The current release (as of mid-September 2026) is version 0.15.8. Scroll down to the **Assets** section > then click on the "Show all 172 assets" link. Scroll down until you find the file named "**tinymist-installer.sh**."



Click on that file to download it. The ".sh" suffix indicates that the file is a shell script. You

will begin by making the script executable. Using your DE's file manager, navigate to the directory where the file was saved and right-click on it. Click on the **Permissions** tab to bring it forward, then check/tick the box next to the **Execute** option.



(Alternatively, you can make the shell script executable via the command line. Open a Terminal/Konsole and issue the command: "**chmod +x tinymist-installer.sh**").

Next, you will run the script to install Tinymist. The script is quite handy and takes care of everything "under the hood" for you. It detects which platform you are on, fetches an appropriate archive from the Tinymist GitHub page, then unpacks the binaries and installs them to the **~/local/bin** directory. It will also add that directory to the \$PATH by adding the appropriate line to your shell profiles.

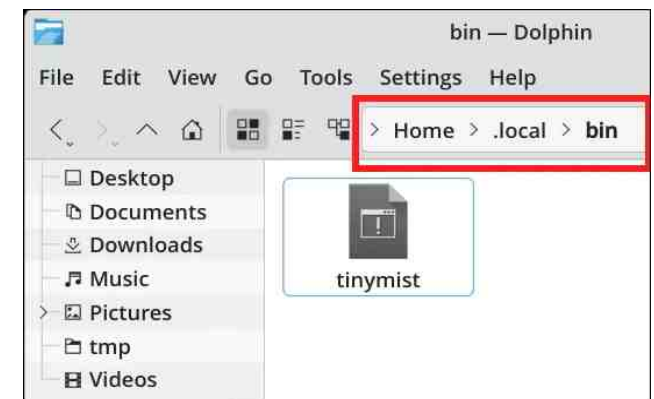
To run the installer script, open a Terminal/Konsole and type **./tinymist-installer.sh**

(You do not need root privileges to run the script. Remember to include the "**./**" at the beginning of the command.)

The installation sequence and Terminal output will look something like this:

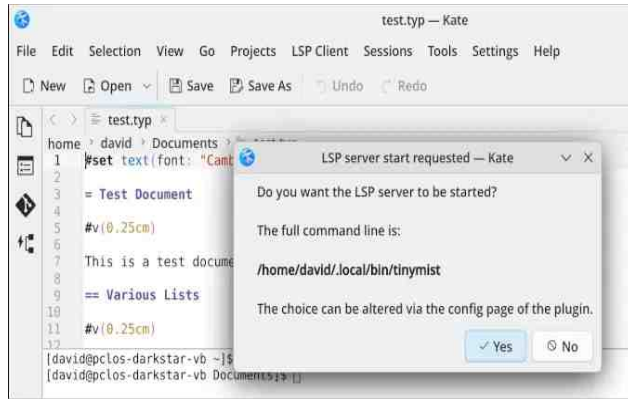
```
[david@pclos-darkstar ~]$ cd
Downloads
[david@pclos-darkstar Downloads]$
ls
tinymist-installer.sh*
[david@pclos-darkstar Downloads]
$ ./tinymist-installer.sh
downloading tinymist 0.15.8 x86_64-
unknown-linux-gnu
installing to /home/david/.local/
bin
tinymist
everything's installed!
```

In PCLinuxOS, the script installs Tinymist to the **~/local/bin** directory:



Restart Kate and open your Typst file, so that Kate can detect the new Tinymist binary. A pop-

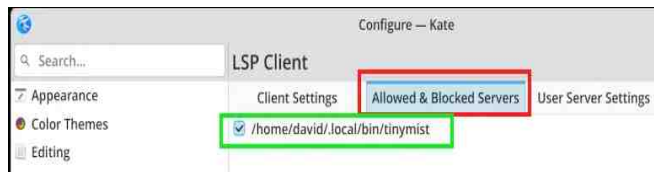
up dialog will appear, asking if you want to start the LSP server.



Click on the "Yes" button. Afterwards, check that the Tinymist language server is working. Look at Kate's **Output** panel; you should see a log similar to the screenshot below.

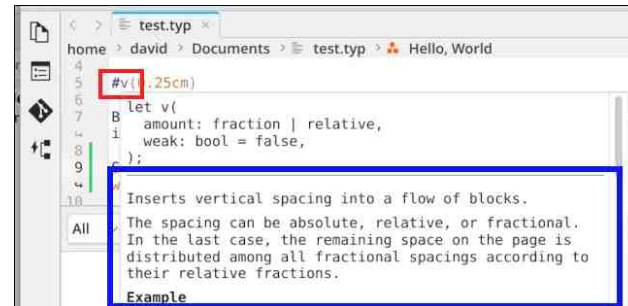
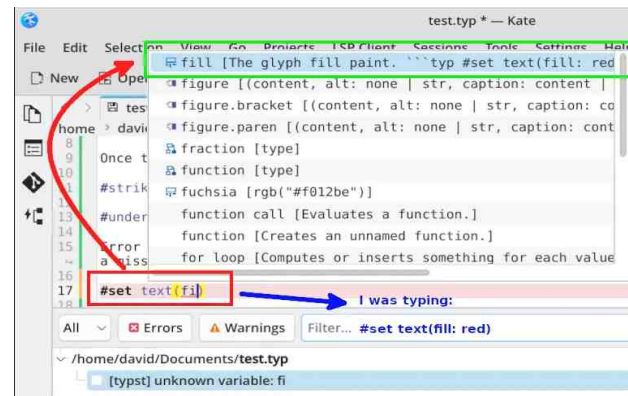


You will also notice that Tinymist is now listed under the **Allowed & Blocked Servers** (Settings menu > **Configure Kate** > **Plugins** section > **LSP Client**):



A Glance at Tinymist's Goodies

Below are two screenshots to illustrate IDE-specific features provided by Tinymist. The first image shows autocompletion in action; the second image shows a tooltip while hovering.



Let's Begin Editing ...

Open your Typst source file with Kate.

(Optional) If your document is in a subfolder with associated image files, and you want to see all the items in a tree display, open it via the **File** menu > **Open Folder ...**

Using Kate's built-in Terminal widget, first generate a PDF file by issuing the command **typst compile your-filename.typ**

Open the Typst-generated PDF with Okular (in a separate window on your desktop).

Leave the PDF Viewer open on your desktop.

Go back to Kate's built-in Terminal widget and issue the command **typst watch your-filename.typ**

You should see output similar to this:

watching main.typ
writing to main.pdf

[00:18:30] compiled successfully in 50.28 ms

The **typst watch** command monitors the input file and its dependencies for changes and automatically recompiles to PDF.

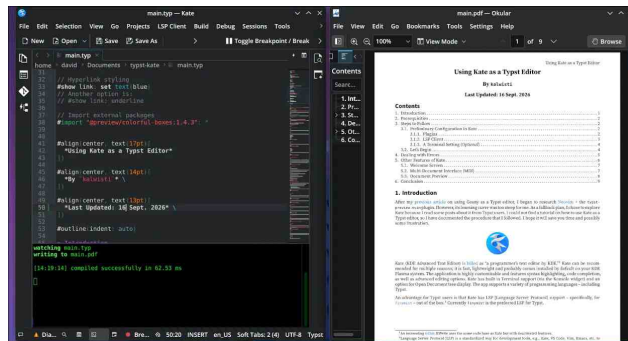
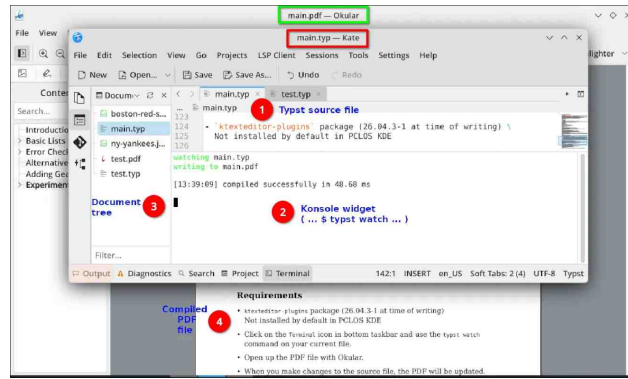
When you make an edit in Kate and save your source file, the PDF will auto-update.

So, you will have two separate windows open (with an asynchronous preview):

1. Kate (with your Typst source file)
2. Okular (displaying the compiled/rendered PDF output)

The screenshots below illustrate how this arrangement looks. (You can toggle between

windows as needed, or position the windows side by side.)



Dealing with Errors

Error messages' formatting will look slightly different, depending on which of Kate's bottom panels is active/focused. The **Terminal** panel displays error messages generated by the **Typst CLI**, while the Diagnostics panel displays error messages generated by the Tinymist language server.

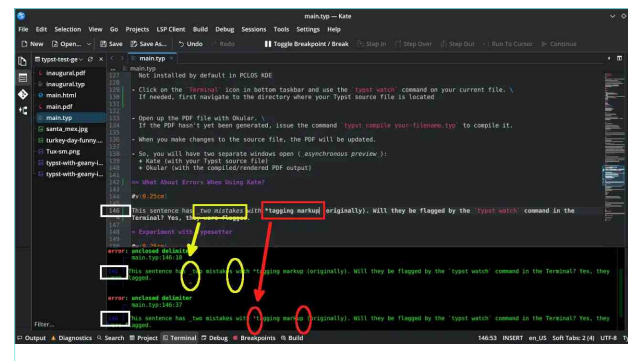
Tip: If you installed Tinymist, Kate's **Diagnostics** panel will simultaneously display any error messages, along with Kate's **Terminal**

panel. You may choose to view whichever panel you prefer — or even jump back and forth between them.

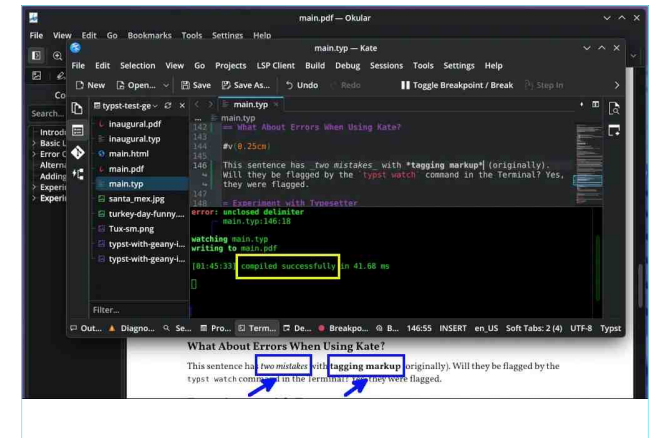
Error Messages via the Typst CLI (in Kate's Terminal Panel)

If you commit a syntax error in your Typst source file, the PDF will not compile. You can then check output in the Terminal widget (where the Typst CLI is running) for detailed error messages about the problem and how to fix it. Based on my testing, the Typst CLI provides slightly more detail than the Tinymist language server.

In the example below, there are two closing delimiters missing. (The Typst source file should read “**two mistakes**” and “***tagging markup***”). I received the message “**compiled with errors**” but the CLI output helpfully indicates the line number (and character positions) of the errors.



Once you have corrected these two minor mistakes and saved your change, the Typst source file will compile successfully to PDF:

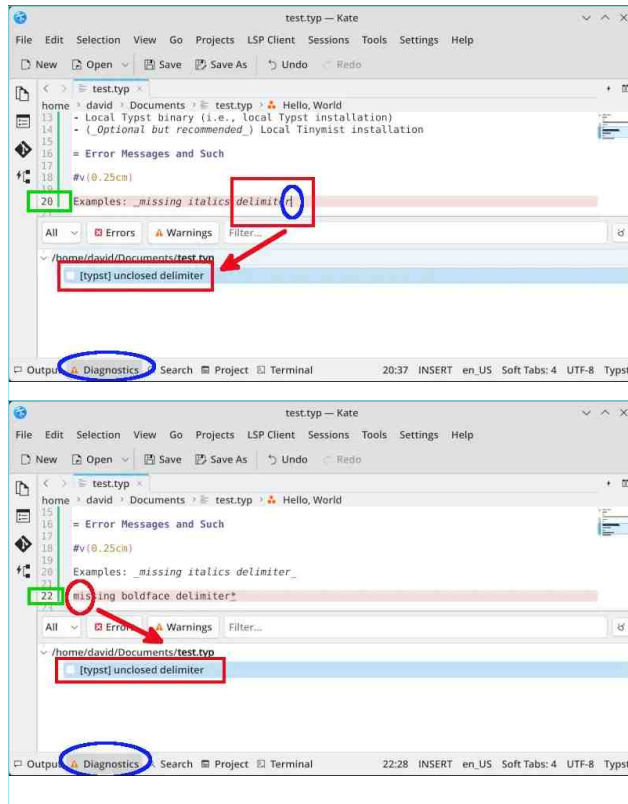


Error Messages via Tinymist (in Kate's Diagnostics Panel)

In the examples below, there are markdown delimiters missing. (The Typst source file should read “**missing italics delimiter**” and “***missing boldface delimiter***”). The **Diagnostics** panel is active because in this editing session, I chose to view the error messages generated by Tinymist.

As we can see, Tinymist's error messages are less verbose than the Typst CLI's messages. Tinymist alerts us that there is an unclosed delimiter; it does not state the line number textually, but the line is highlighted in pink in Kate's main Editor pane (next page).





Other Features of Kate

Kate has many useful features worth exploring. The *Kate Handbook* is an excellent guide with detailed information which you can access by pressing the F1 function key, or via the **Help** menu > **Kate Handbook**.

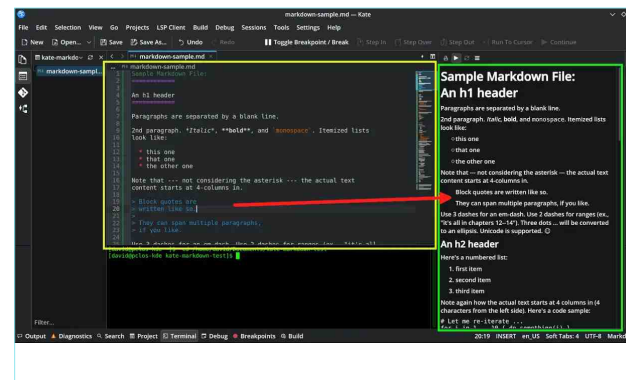
Document Preview

Although the technical details are mostly beyond my grasp, I will attempt to explain why this functionality is currently lacking for Typst files. Real-time document preview requires

writing a dedicated, separate KParts viewer plugin. **KParts** is a KDE component technology that allows applications to embed and use dynamically loadable modules for various functionalities, such as document viewing or editing.

This plugin for Typst files [has not yet been written](#), so no real-time preview is possible at the moment. However, if/when a Typst viewer plugin is created, it would likely be similar to the Markdown Viewer KPart (shown below in action).

Tip: To preview markdown files in Kate, you must install the **markdownpart** package from the PCLinuxOS repositories.



Conclusion

Editing Typst files with Kate was an enjoyable experience. I prefer it over the [Geany editor + Typst](#), and perhaps even more than the combination of [VSCodium](#) and [Typst](#). If KDE Plasma is your favorite desktop environment, I encourage you to try editing your local Typst files with Kate. You might well find this

workflow more productive than editing with VS Code/VSCodium.

I am on the fence about the distraction level of Tinytist's autocompletion feature. I intend to experiment with it a bit longer before making a final decision. My ambivalence is due to the fact that I became accustomed to checking Typst's [online documentation](#) when I am uncertain about syntax. If you choose not to install the Tinytist language server, another viable option is to download the [print version](#) (PDF, 692 p., 26 MB) of Typst's documentation for release 0.15.1 and to consult it offline.





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

PCLinuxOS Magazine,
send an email to:
[**pclinuxos.mag@gmail.com**](mailto:pclinuxos.mag@gmail.com)

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

The High Crime Of "LMAO": How Cops Are Treating Flock's Mass Surveillance As A Joke



Image by EFF (CC-by)

by [Rindala Alajaji](#) and [Dave Maass](#)
[Electronic Frontier Foundation](#)
Reprinted under Creative Commons [license](#)

Here's a riddle: Why did a Goshen Police Department officer search 6,474 automated license plate reader (ALPR) networks, representing data from 82,413 cameras, on May 7, 2025?

If your answer is "I don't know," it turns out you're 100% correct. The officer left the letters "idk" in the search field where cops are supposed to document the reason for the search.

When law enforcement and tech salespeople pitch ALPRs to city councils, they stick to a familiar script. They trumpet the technology, which is often provided by private companies like [Flock Safety](#), [Motorola Solutions](#), or [Axon](#), as an essential tool for solving high-stakes crimes, such as car jacking, kidnapping, or murder.

But when you strip away the carefully [curated talking points](#), the data continues to reveal a different (and frankly, ridiculous) story. An EFF analysis of ALPR search logs from Flock Safety systems shows that officers across the country are spying on drivers for completely

nonsensical "reasons." Police are routinely searching the Flock database without providing any legitimate justification, making a mockery of our civil liberties by logging reasons like "LOL" (short for "laugh out loud"), "LMAO" (short for "laughing my ass off"), "sexy," and "idk" (short for "I don't know") to access sensitive ALPR location data.

And in some cases, officers are just mashing keyboard buttons rather than articulating the nature of their searches.

Flock Safety claims it has improved its system by requiring officers to select from a [dropdown](#) list of crimes before running a search – but that only makes it easier for officers to hide improper searches behind the veneer of uniformity. The system does not require proof that the dropdown reason actually matches the true purpose of the search.

With no warrant requirements, limited guardrails, and deficient audit processes, ALPR databases have fostered a culture of unrestricted access to everyone's location information. This culture of abuse has allowed police to treat a mass surveillance network like their own personal search engine, permitting the tracking of the movements of everyday citizens for [low-level complaints](#), [personal whims](#), and sometimes, seemingly, [for the lols](#).

The High Crime Of “LMAO”: How Cops Are Treating Flock's Mass Surveillance As A Joke

A Documented Culture of Abuse

ALPR misuse isn’t a new phenomenon; it has dominated headlines for more than a year. We already know that officers regularly abuse these systems to stalk past and potential romantic partners. We’ve seen ALPRs used to surveil protests, which can chill First Amendment-protected dissent, and seen officers try to use an ALPR system to track down a woman seeking an abortion.

Typically, we learn about these uses from documents called "network audits," which are long spreadsheets that document all the searches that run through an agency's system. It is not unusual for even a small agency to have a record of millions of searches from thousands of external agencies across the United States.

We’ve also uncovered horrific systemic profiling, with more than 80 law enforcement agencies using terms like "roma" and "g*psy" to target ethnic Romani people—often without any mention of a suspected crime. And when police aren’t using ALPRs for stalking or profiling, they routinely use them for extreme low-level investigations: verifying whether a student lives in a specific school zone, running employment background checks, following up on loud music complaints, or targeting a motorcyclist simply for holding a cell phone.

But somehow, it gets worse.



Name	Org Name	Total Networks	Total Devices Searched	Time Frame	Reason
B. McK	Lake County IN	1558	19592	07/09/2025, 01:00:00 PM UTC 07/11/2025, 03:00:00 PM UTC	LMAO
B. McK	Lake County IN	1558	19592	06/11/2025, 03:00:21 PM UTC 07/11/2025, 03:00:21 PM UTC	LMAO
B. McK	Lake County IN	1558	19592	06/11/2025, 03:00:21 PM UTC 07/11/2025, 03:00:21 PM UTC	LMAO
B. McK	Lake County IN	1558	19592	06/11/2025, 03:00:21 PM UTC 07/11/2025, 03:00:21 PM UTC	LMAO
B. McK	Lake County IN	1558	19592	06/11/2025, 03:00:21 PM UTC 07/11/2025, 03:00:21 PM UTC	LMAO
M. Ess	Barberton OH PI	409	6779	02/10/2025, 06:00:45 AM UTC 02/12/2025, 06:00:45 AM UTC	lol
M. Ess	Barberton OH PI	409	6779	02/08/2025, 06:00:00 AM UTC 02/12/2025, 06:00:45 AM UTC	lol
M. Ess	Barberton OH PI	410	6797	02/11/2025, 06:00:16 AM UTC 02/13/2025, 06:00:16 AM UTC	lol
M. Ess	Barberton OH PI	410	6802	02/13/2025, 05:30:53 AM UTC 02/14/2025, 05:30:53 AM UTC	LOL
M. Ess	Barberton OH PI	411	6813	02/20/2025, 03:30:01 AM UTC 02/20/2025, 05:30:01 AM UTC	lol
M. Ess	Barberton OH PI	418	6950	03/14/2025, 09:00:37 AM UTC 03/16/2025, 09:00:37 AM UTC	LOL
M. Ess	Barberton OH PI	418	6986	03/24/2025, 04:00:01 AM UTC 03/24/2025, 06:00:01 AM UTC	lol

Audit logs sample

The Absurdity of Documented Search Reasons

EFF’s analysis of Flock Safety’s ALPR search data obtained through public records requests has uncovered a disturbing trend. In the absence of judicial oversight, officers are inputting ridiculously unserious terms to justify their searches. Here is just a snapshot of what police consider a "reason" to track someone’s vehicle:



Surveillance as a Joke

Barberton Police Department (Ohio) employees ran numerous searches between March 2024 and May 2026, listing “LOL” or “lol” as the reason.

Harris County Sheriff's Office (Texas) employees ran several searches between April and May 2026 listing “LOL” or “lol” as the case number.

Lake County Sheriff's Department (Ind.) employees ran searches in July 2025 for “LMAO.”



The High Crime Of “LMAO”: How Cops Are Treating Flock's Mass Surveillance As A Joke

Richmond Police Department (Calif.) employees ran over multiple searches in November 2024 for “**Hehe.**”

Riverside County Sheriff's Department (Calif.) employees ran searches in 2024 for “Haha.”

"Don't Know, Don't Care" Approach

Kankakee County, Sheriff's Office (Ill.) employees ran searches (2023–2025) for “**idk**” or “**idk lol.**”

Goshen Police Department (Ind.) ran searches (May–June 2025) for “**idk.**”

Fishers Police Department (Ind.) ran searches in May 2025 for “**blah.**”

A Pasco Police Department (Wash.) employee searched for at least four different license plates, leaving “**robbery i don't remember the case number leave me alone**” in the reason field.

The San Diego Sheriff's Department (Calif.) ran searches in May 2025 with “**idk**” in the reason field.

More than 30 agencies ran more than 6,300 searches with “**TBD**” (short for “To Be Determined”) as the “reason.” These included the Arizona Department of Public Safety, the Manteca Police Department (Calif.), and the Baton Rouge Police Department (La.). The Priceville Police Department (Ala.) alone ran 1,954 searches with reasons “TBD.”

Insults and Inappropriate Searches

Belton Police Department (Mo.) ran searches (Aug–Sept 2024) for “**d*ckhead.**” (asterisk/redaction our own)

A Manteca Police Department (Ill.) employee ran searches in June 2024 for “**sh*thead**” (asterisk/redaction our own)

A Norton Police Department (Mass.) employee ran searches in December 2024 for “**Sexy.**”

Corona Police Department (Calif.) employees ran searches (2023–2025) for “**weird**” or “**WEIRD KID.**”

Thornton Police Department (Colo.) employees ran several searches in October 2025 for “**driving around being weird.**”

A Columbus Police Department (Ohio) officer ran searches in 2023 for “**idiot.**”

A Michigan City Police Department Officer (Ind.) ran searches in June 2025 listing “**f*ck this new search engine.**” (asterisk/redaction our own)

Button Mashing

One of the more alarming discoveries we found in the network audit data is a large number of “reasons” that appear to be nothing more than an officer mashing buttons. These typically involve a nonsensical long string of characters from the same line or area of the keyboard.

For example:

An Eatonton Police Department (Ga.) employee ran searches with reasons such as **HJKNUILH**,

Name	Org Name	Total Networks Searched	Total Devices Searched	Time Frame	Reason
A. Hyl	Gwinnett County GA PD	976	16057	03/14/2025, 03:30:00 PM l 04/13/2025, 03:30:00 AM l	hjhjhkh
B. Whi	Moore OK PD	6492	83155	04/15/2025, 11:00:28 AM l 05/15/2025, 11:00:28 AM l	ghjhghjg
D. Lee	Kansas City MO PD	637	10783	04/17/2025, 06:30:55 PM l 04/17/2025, 08:30:55 PM l	fhjhj
L. Eri	Brown County WI SO	418	6636	06/25/2025, 11:00:12 AM l 06/25/2025, 01:00:12 PM l	ho:hjhjhj.jklqegsdfzsagfdasfkl
L. Eri	Brown County WI SO	392	6714	07/13/2025, 06:00:01 AM l 07/13/2025, 06:00:01 PM l	HJHJKLHLKHJK
L. Joh	Atlanta GA PD	990	16643	12/4/2024, 11:00:25 AM U 12/6/2024, 11:00:25 AM U	HJHKJ
M. Day	Kentucky State KY PD	6502	81043	03/23/2025, 03:56:03 PM l 04/22/2025, 03:56:03 PM l	dghjhghf
M. Luj	Ector County TX SO	458	8195	2/9/2025, 08:00:46 PM UT 2/10/2025, 08:00:46 PM U	bhhjh
A. Hyl	Gwinnett County GA PD	948	15509	03/04/2025, 01:00:58 PM l 03/07/2025, 01:00:00 AM l	1kkkjju;
L. Bri	Sacramento County CA SO	344	5583	06/04/2025, 02:30:23 PM l 06/04/2025, 04:30:23 PM l	wertyui

Button mashing audit logs sample

The High Crime Of “LMAO”: How Cops Are Treating Flock's Mass Surveillance As A Joke

uiokjk.kuj, GJLHBNMN, hjhbnmg, and iuhjck.

An Atlanta Police Department (Ga.) employee ran searches with **asdfga** as the reason.

Bay County Sheriff's Office (Fla.) employees ran searches with reasons such as **;'lkjh, /lkjh** and **lkjhg**.

A Brown County Sheriff's Office (Wis.) employee ran searches with reasons such as **gyghkkghghjkgghjk, ggyjgyujdsrdghdfhjkgghjghk, HJHJKLHLKHJK, hjjkjkhjkljk** and **JHLJKHHJKL**.

A Lake County Sheriff's Office (Ohio) employee ran searches with reasons such as **asdfg** and **ghjkl**, and a second officer ran a series of searches that started off with "investigation" but then devolved into button mashing, including:

Investigatafy, Investigatafyd, Investigatafydl, Investigatafydlh, investigatafydlhj, investigatafydlhji, investigatafyfdlhji, investigatafyfdlhjigkfgty, investigatafyfdlhjigkfgtyy, investigatafyfdlhjij, investigatafyfdlhjik, investigatafyfdlhjikf, investigatafyfdlhjikfg, investigatafyfdlhjikfgty, investigatafyfdlhjikfgy and investigatafyfdlhjiy.

A Moore Police Department (Okla.) ran searches with reasons such as **jhjhkhjh, jhkhkhjh, jkhhkhjh, Jkhkhjh,**

Jkhkhjh, Jkhkhjhkh, jkhkhkhjh, jkhkhjh, kjkhjh, loiuiou, ukjhkh and ulkuuiou.

A Westlake Police Department (Ohio) employee ran searches with reasons such as **fghjkl, ghjkl, and lkjhg**.

A Kentucky State Police employee ran searches with reasons such as **mhghjk, mhgnhjck, nbvcxcvbn, nmbvcbnm, and sdfghj.**

It's hard to imagine a situation where these characters add up to a legitimate police code. However, it's easy to imagine an officer cutting corners with a text field they know no one is checking, especially if they are accessing the Flock Safety app from their phones while driving.

How Police Departments Are Responding

When confronted with these flagrantly unserious searches, police departments offered a mix of bureaucratic deflections and excuses.

In response to EFF's request for comment, Thornton Police Department (Colo.) claimed the system didn't require officers to select from a defined list at the time, but it does today. They also audited the “driving around being weird” searches, claiming they were all actually for “legitimate public safety purposes.”

Other police departments we reached out to for comment shared the following:

Richmond Police Department (Calif.) stated that the officers involved with the "Hehe" and "idk" searches were "counseled."

Corona Police Department (Calif.) noted that the employees searching for "WEIRD KID" are no longer employed by the city for unrelated reasons.

Columbus Police Department (Ohio) pointed to their union contract, stating their Inspector General only has jurisdiction to investigate incidents within the last 90 days, giving the officer who searched for "idiot" in 2023 a free pass.

Belton Police Department (Mo.) promised a "thorough investigation" of the "d*ckhead" searches through existing union and personnel policies.

Manteno Police Department (Ill.) said it will "review the searches and the circumstances surrounding them thoroughly" and "take whatever action is determined to be appropriate based on the facts and circumstances."

Manteca Police Department (Calif.) said: "Since the beginning of 2026, our personnel have been directed that the reason field for ALPR searches must identify the law enforcement purpose for the search and that 'TBD' is not an acceptable entry." The spokesperson added: "The presence of 'TBD' in the reason field in prior searches should not, by itself, be interpreted to mean that the associated search was conducted without a legitimate law enforcement purpose or that reasonable suspicion was required." EFF has

The High Crime Of “LMAO”: How Cops Are Treating Flock's Mass Surveillance As A Joke

asked the agency to clarify whether it verified the hundreds of “TBD” searches were legitimate, and we will update this post with a response if we receive one.

Fishers Police Department (Ind.) said that the detective that searched for “blah” has done so “when he has issues with the technology” and that the term “is used when he is actively using the technology to solve a criminal case, and the technology is not moving fast enough for him.” The department shared that “he has been told to use “test” in the future.”

The Cobb County Police Department (Ga.) acknowledged that “TBD” stood for “To Be Determined” and is no longer an acceptable search reason: “We have instituted a new policy that took place after the dates listed in your audit that now require, in addition to a criminal offense and a reason, a case number for any search conducted on FLOCK.”

The San Diego County Sheriff's Department says that it checked the cases where “idk” was used and determined “there was an active investigation associated with the searches.” The department said that this was due to the reason field being optional at the time (which was true on a software level) but California law has required officers to document a purpose for accessing ALPR data since 2015. The sheriff's spokesperson says the reason field is now mandatory, and involves a dropdown menu.

Other agencies did not respond to EFF's requests for comment. We will update with responses as they are received.

The Cop Out of the Drop-Down Menu “Feature Update”

Under the guise of streamlining audit logs, in late 2025, Flock safety [announced](#) that they will be replacing the required, free-text search “reasons” with a pre-populated dropdown menu of generic offense categories. Since this update, officers are no longer required to type out why they are digging through a driver's movement history, and instead can select a pre-packaged option like “Traffic infraction” or “Other” in half a second.

Replacing the requirement to articulate the reason for the search with one-click searches is a loss for transparency, but also may explain why audit logs including the searches we highlight in this piece significantly decreased since early 2026.

The Punchline is Our Privacy



Entries like these defeat transparency, undermine accountability, and entirely fail to satisfy what many jurisdictions require by law

or policy: an actual reason for the search. And this keeps happening because police use ALPRs as a convenient shortcut around constitutional privacy safeguards.

In other contexts, such as searches of [cell phone location information](#), police have to go to a judge, demonstrate probable cause, and get a search warrant. But because laws and courts have not caught up with the pace of ALPR technology, police do not do the same before searching ALPR databases. Instead, they are given free rein to track a person's movements without a sliver of judicial oversight.

As we [mention](#) in our piece about the use of ALPR surveillance for low-level investigations, if a police chief stood in front of a city council and asked for permission to install hundreds of cameras just so his officers could investigate the high crime of “haha,” they would be laughed out of the room. The same could be said if an officer asked a judge to sign a warrant to track someone down for “LOL.”

The fact that these searches were not only missed by the agency supervising the officer, but by the often thousands of other agencies whose systems were searched, demonstrates how agencies cannot be trusted to oversee themselves.

Mass surveillance is incompatible with a free society, and especially so when the people with access to this data are treating it like a joke. This ALPR mass surveillance—the indiscriminate, continuous collection and retention of location data on every driver, regardless of suspicion—

The High Crime Of "LMAO": How Cops Are Treating Flock's Mass Surveillance As A Joke

should not exist. But because it does, EFF continues to urge courts and state legislatures to immediately step in and impose strict, enforceable restrictions to rein in this abuse. At an absolute minimum, this means mandating rigid data deletion deadlines and an ironclad warrant requirement.

If police want the power to track a person's movements, they must be required to convince a judge with evidence and probable cause. They should not be able to bypass the Constitution with a search for "haha."

Additional Reading About The Flock Drama From EFF:

[Cops Play Hide and Seek About Using Spy Tech to Avoid Scrutiny and Bad PR](#)

[Texas and Florida Step Back from ALPRs](#)

[EFF's Policy Position on ALPR Surveillance: Eliminate It and Reduce Its Harms](#)

[Too Little, Too Late: Flock Admits Their Technology Needs Reforms](#)

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

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

The **PCLinuxOS** magazine



Screenshot Showcase



Posted by Meemaw, September 1, 2026, running Xfce.

All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads

by Paul Arnote (parnote)

Last month, I wrote about how to use mpv to watch OTA television broadcasts. This month, let's talk about how to record OTA television broadcasts via your TV tuner card, and then how to edit out the ads or commercials.

As I stated last month, mpv has become my go-to tool for *watching* OTA television broadcasts. But, for recording those OTA television broadcasts, it's hard to beat Kaffeine for ease of use.

To get started, you will need to install Kaffeine and Avidemux. The latter is installable from the PCLinuxOS repository via the DNF Package Manager. As for the former, I'm using the Flatpak version of Kaffeine. Of course, you will also need a TV tuner card. Mine is a KWorld KW-UB435-Q V3 USB TV tuner card, and it works perfectly. I picked mine up from eBay for a pretty low price.

My USB TV tuner card is "old stock," and no longer manufactured (in a stroke of luck, I did manage to pick up a "spare" a few years ago when I found one new in the box listed on eBay). Thus, any you find on eBay will likely be used/preowned, and may be difficult to locate. There are a few USB [TV tuner cards](#) I found on eBay, but I'm unsure if they work with Linux. If you have the funds, it might be worth giving them a try, as they run in price between \$20 and \$40 (U.S.). If you do give them a try, let me know how they work, or if they work.

I have purchased one (the first one I linked to), and I'll let you know how it works after I receive it. (**Note:** it does not work in my area. That particular USB tuner card and the second one I linked to are for DVB-T, which is the digital TV standard for Europe. Since I'm in the U.S., I need a USB tuner card that works for ATSC/QAM. I have ordered another USB TV tuner card that is compatible with the broadcast standard in my area,

which is the third USB TV tuner card I linked to above.) That first linked USB tuner card (running right around \$20 U.S.) does have some reports of working decently under Linux, provided DVB-T is the broadcast standard for your area.

If you don't already have Kaffeine set up to display OTA television broadcasts, I wrote about how to configure Kaffeine to display OTA television broadcasts in the [September 2022](#) issue of The PCLinuxOS Magazine. I'll refer you to that article to get your copy of Kaffeine configured for the OTA television broadcasts that are in your area.

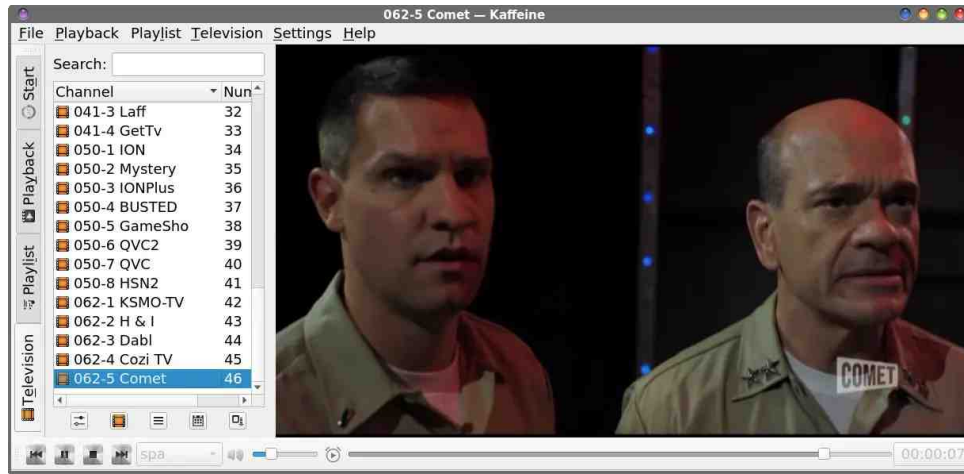
Recording Your Show



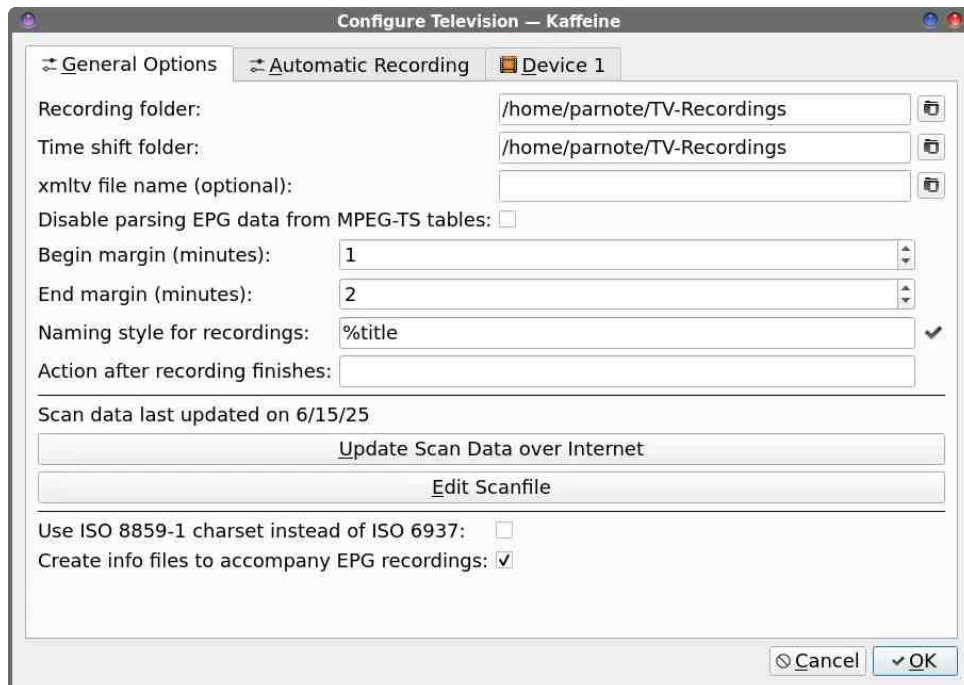
The screenshot above shows what Kaffeine looks like when you first launch it. You'll want to select the "Digital TV" button to display OTA television broadcasts in Kaffeine.



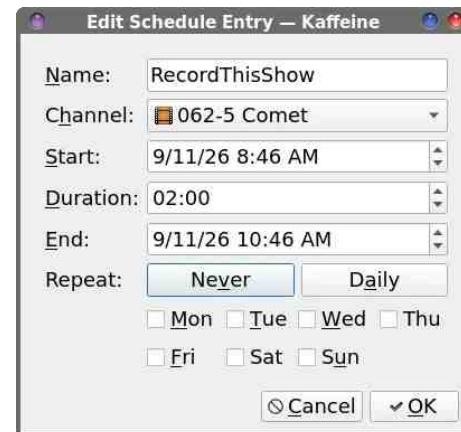
All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads



Next, find the channel that has the program you want to record. Here, for demonstration purposes, I'm displaying the local channel where I live that airs the Comet station.

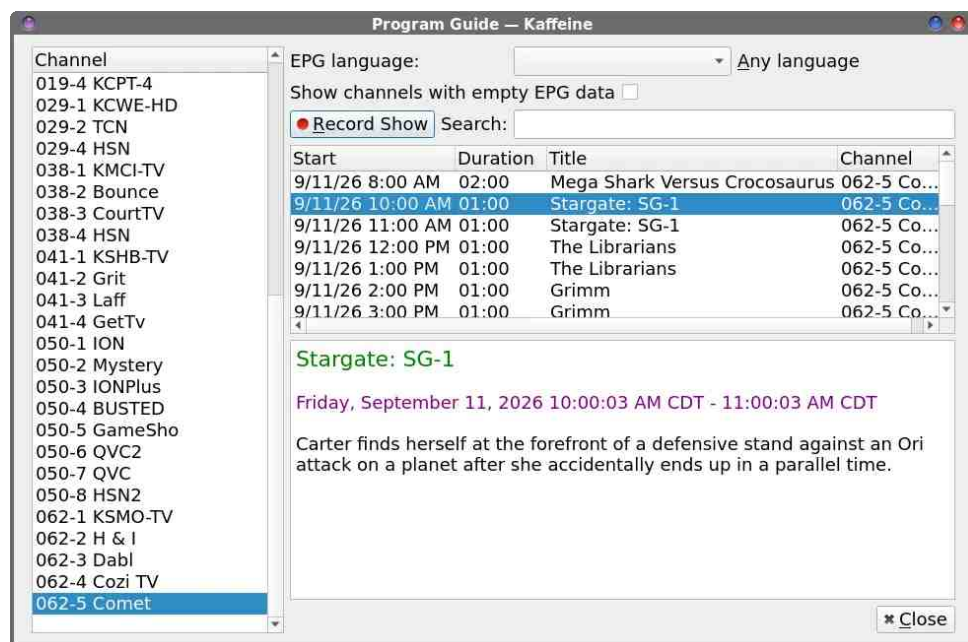


It would be a good idea to set up some settings for recording OTA television broadcasts. Under the “Television” menu, select “Configure Television ...”. There (as shown in the screenshot at the bottom of the previous column), you can set up where you want Kaffeine to save your recorded files. I make my “Time Shift” directory the same as my “Recording” directory. I have a “special” directory that is a top-level directory under my /home directory, that I call “TV-Recordings.” Then, I set the “Begin margin” setting to one minute, and the “End margin” setting to two minutes. This causes Kaffeine to start recording one minute before the show that I want to record starts, and continues for two minutes after the scheduled end of the show I want to record. By doing this, you only have to “worry” about entering the actual time your program starts.

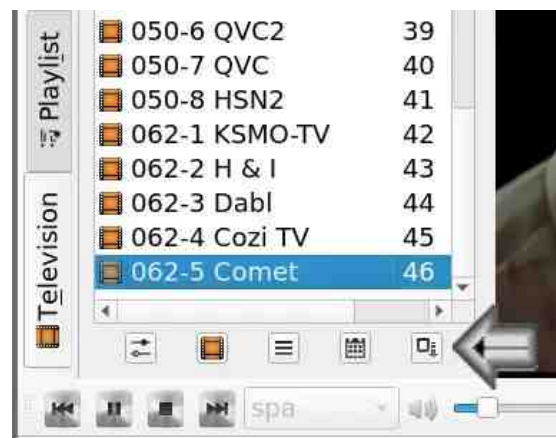


All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads

There are a few different ways to tell Kaffeine that you want to record a program. The first way is to go to the “Television” menu, and select “Recording Schedule” (first image immediately above). Click on the “New” button, and a dialog box similar to the second image shown above will appear. Give the recording a “name,” and then select the channel you want to record. Then, set the start date and time, as well as the duration of the program. I like this method best, since it gives you the opportunity to specify a unique name for the recorded file.



Another way is to record your program from the Program Guide in Kaffeine. To access it, go to the “Television” menu, and select “Program Guide” from the menu. Now, select the program you want to record from the list of programs, and hit the “Record Show” button (top left of the right window pane). Once you hit that button, a small red “dot” will appear in front of the selected program, to indicate that program will be recorded to your hard drive.



Of course, the third way to record a program with Kaffeine is to hit the “Instant Record” button (right-most button immediately under the channel list). I have to admit that I almost never use this button, but it should keep recording until you hit the button a second time (or until you run out of disk space ... recording video takes up a LOT of hard drive space!).

If you want or need to provide a unique name to a recorded file using the second or third method of setting up a program to record, you can go back to the “Recording Schedule” dialog box, and edit the scheduled recording to have a more unique name.

Keep in mind that you will need to keep Kaffeine running after setting up your recording, regardless of which method you use to set up a recording. For me, sometimes the show I want to record is on at some time when I’m not in front of my computer, like when I’m doing “other” things during my waking hours, or when I’m sleeping. But, Kaffeine needs to already be running to record your program. So, for those times, I just turn the volume all the way down in Kaffeine and minimize the Kaffeine window to my panel.

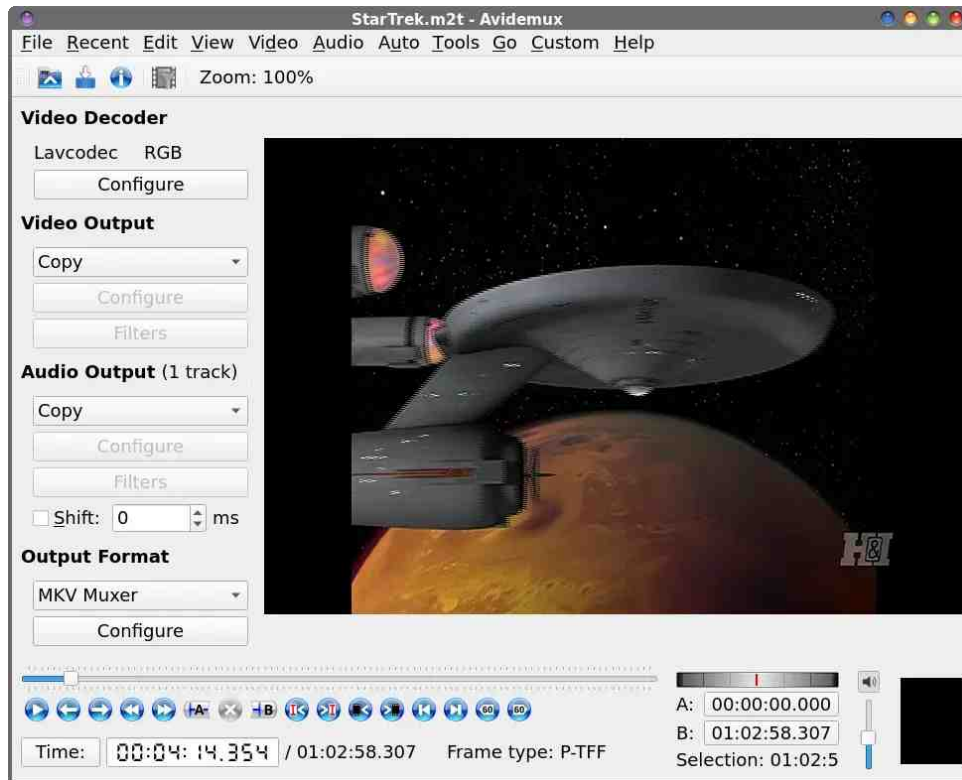
So now, at the selected time, Kaffeine will save your selected OTA broadcast to the folder you specified. The file will be saved as a *.m2t file, which stands for MPEG-2 transport stream. It will be given the name you specified (if you used the first method to set up your recording), or the name of the program as it appears in the Program Guide (if you use the

All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads

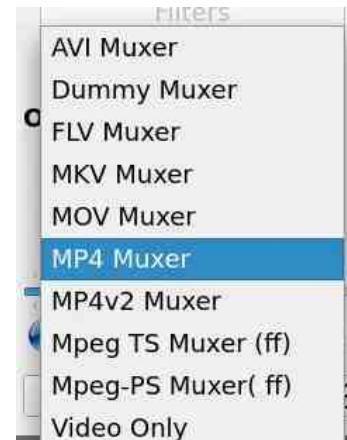
second or third method to set up your recording, and you haven't edited the name to provide a more unique name for the file).

Let's Get Rid Of Those Annoying, Inane, Pesky Ads

Once your recording is done, it will be stored in the directory where you told Kaffeine to store your programs. So, go to that directory and find the program you just recorded.



Load the *.m2t file produced by Kaffeine into Avidemux. You should see something like the screenshot above. While I'm certain that there are other capable video editors out there, I like using Avidemux, which is a very capable frame-based video editor that's super easy to use (there are time-based video editors, which aren't nearly as precise or as good at making clean edits).



Leave all of the settings (Video Decoder, Video Output, Audio Output) to their default values. The only thing you might want to change is the "Output Format" setting. While I have nothing against MKV files, I'm more comfortable working with MP4 files, so I changed the output format to MP4.

Just to be sure that you're working from the very first "frame" of the recorded video file, I like to grab the slider control with my mouse, and then move it to the right, and then all the way back to the left ... which should represent the first "frame" of the video.



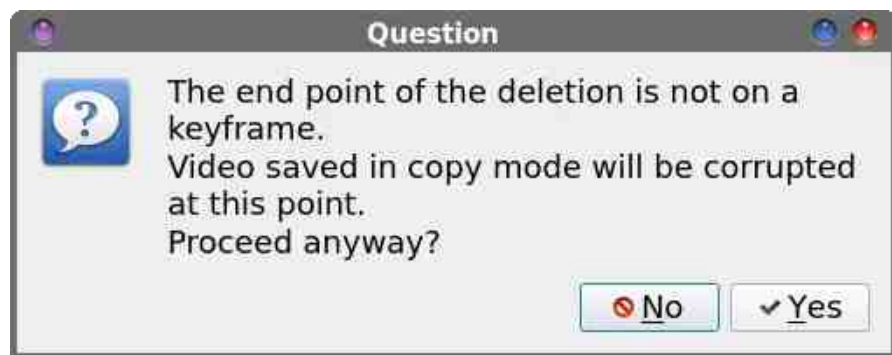
Now, you can use the cursor keys on the keyboard of your computer to navigate through the video.

Tip: pressing the Ctrl key + the left or right cursor keys will move through the video at 2X speed, which makes finding the correct "cut points" in the video much easier.

All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads

There are typically “dissolves” between the program you’re wanting to keep and the ads. Heck, there are even “dissolves” between the ads. Using the cursor keys (or even the Ctrl + cursor keys), you can rapidly move through the video to find the ads. Find a frame where it dissolves to black between the end of the program segment and the start of the ad, and press the “A” (black arrow in the image above) to set the first cut point. Then, find a black frame immediately before your program restarts after the ads, and press the “B” (blue arrow in the image above) to set the second cut point. Then, the “X” button (red arrow in the image above) should be red. Select it, and the first set of ads will be deleted. The ability to set the A and B marks also exist under the “Edit” menu, if you prefer using the menu instead of the buttons on the toolbar.

Tip: there are other key combinations that offer different rates for moving through the video. To see them, select the “Go” menu in Avidemux. They are listed as the last eight menu options under the “Go” menu.



The first time you cut out a section of ads, you’re likely to see the dialog box shown above. Go ahead and say “Yes” to this question. Honestly, I have yet to notice any corruption or degradation in the resulting video file. Every compressed video codec contains a pattern of an “I” frame, and each “I” frame is followed by two “B” frames and one “P” frame in a repeating pattern until the next “I” frame. This pattern repeats until the end of the video. You’ll likely see this message if one (or both) of your “cuts” is NOT on an “I” frame. “I” frames contain a full image, and serve as a reference frame for the other frames. “I” frames are also called keyframes. A “P” frame stores only the changes from the previous frame, and relies on the last “I” frame or “P” frame to reconstruct the image. “B” frames use data

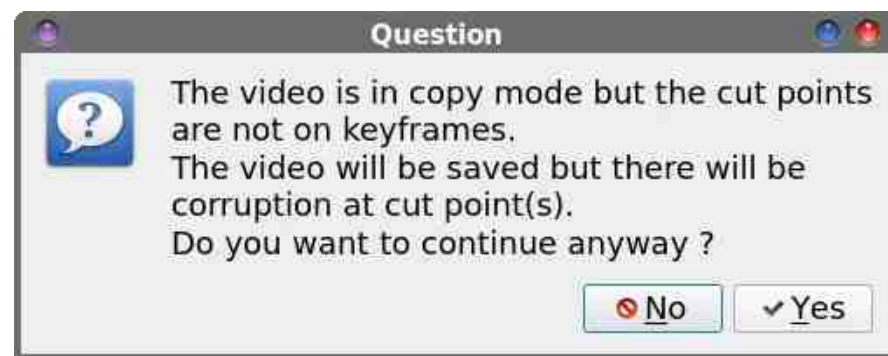
from both previous and future frames, and can reference both “I” frames and “P” frames. They are bidirectional (hence, the reason they are called “B” frames), and are what are responsible for higher compression rates while maintaining video quality.

Repeat these steps of marking the A and B marks, followed by the red “X” button, to cut out the ads for the duration of the video. For a one-hour video, I can accomplish this in less than 10 minutes.

Tip: if you set the “A” mark and DO NOT set the “B” mark, the rest of the video to the end will be deleted just by pressing the “X” button.

Don’t worry if you mess up on setting your A and B marks. At the worst, all you’ll have to do is start over with the *.m2t file. I occasionally find myself having to do the same from time to time. But, the process is relatively fast, so it’s not usually a huge deal.

Once you have your video prepared and devoid of the mindless, annoying, pesky ads, select the “File” menu, and select “Save” from the menu options. Don’t worry ... your recorded video won’t be overwritten unless you just insist that it does so. I guess what I’m trying to say here is that you have to work to make your new video overwrite your original recording.



You may get a similar “warning” about video corruption as we saw in the last message. Ignore it, and select “Yes.” You’ll then be given an option to save the file with the filename of your choice, in the directory you choose. If you’re following along and also changed your Output Format to MP4,

All The Tools You Need To Record OTA TV Broadcasts & Edit Out The Ads

you'll notice that Avidemux will be saving your new file with a MP4 file extension. If you opted for MKV file output, your new file will be saved with a MKV file extension.

Optionally, if you choose, you can play back the resulting video in Avidemux, just to make sure your edits are working as they should. I've done this enough times that I now trust the procedure, so I rarely check these days.



A screenshot from one of the Star Trek episodes I recorded using the method described in this article.

Summary

So why would I (or anyone) do this? Well, for me, it's because I can. Recently, the H&I channel (Heroes & Icons) had a marathon broadcast of

the original Star Trek series to commemorate the 60th anniversary of the release of Star Trek. I'm not a dyed-in-the-wool Trekker, but I do have some favorite episodes that I never get tired of watching. So, the marathon broadcast gave me a chance to grab those episodes. In rewatching them, I didn't want to have to sit through all of the annoying ads again ... and again ... and again ... so it made perfect sense (to me, anyways) to make a copy of those episodes **without** having to sit through those ads every time I choose to watch them.

On a personal note, ST-TOS (Star Trek: The Original Series) isn't necessarily my favorite of the Star Trek universe or franchise. That honor falls to ST-ENT (Star Trek: Enterprise) and ST-VOY (Star Trek: Voyager), in that order. In fact, I watch these two series every night, six nights a week, before I go to bed. It's after the kids go to bed, so this is dad's "unwinding" time from the stresses of the day.

I can think of other reasons why others might want to do something similar. One that comes up repeatedly in my mind is someone who might want to economically (a.k.a. cheaply) build a collection of some of their favorite TV programs. Hey, I get it. Things are expensive these days, so buying DVDs or BluRays isn't necessarily a cheap option. And, with every entertainment outlet looking to sell you streaming packages, those can get pretty expensive, pretty fast. Using this method, you can economically build your OWN collection. The only "investment" you have is your time and the "wear and tear" on your equipment.

But trust me: this whole process is much simpler than it sounds. Describing the process makes it appear to be a daunting task, which is the furthest from the truth. So, don't hesitate to try your hand at this, too!

TorrentFreak

The place where breaking news,
BitTorrent and copyright collide

Secure Messaging & AI Remain In Conflict Despite The Promise Of TEEs



Image by EFF (CC-by)

by [Erica Portnoy](#) and [Thorin Klosowski](#)
[Electronic Frontier Foundation](#)
Reprinted under Creative Commons [license](#)

Secure messaging platforms, like Signal, WhatsApp, and recently, [encrypted RCS](#), operate on a straightforward assumption: the content at each end of a conversation is private to the participants in the conversation. End-to-end encryption helps provide the mathematical guarantees that the companies who operate these messaging platforms cannot access the contents of messages. But there's no way to guarantee

what happens once the message arrives on a phone. As more devices and services introduce more artificial intelligence (AI) features into messaging apps, that line begins to blur.

When AI features are computed entirely on device, it's less concerning. Yet sometimes the computing requirements are heavy enough that the computation has to be done on a company server. Tech companies tell us they have a solution for this: trusted execution environments (TEEs). But do server-side TEEs really solve the problem?

TEEs exist to serve many different functions, ranging from digital rights management (DRM) content protections to securely storing information in your phone's mobile wallet, but for our purposes, we'll be focusing on how tech companies use them for their AI tools.

The basic idea is straightforward: most consumer devices aren't powerful enough to handle the sorts of AI features companies want to offer, so sometimes they send data off your device to more powerful cloud servers to do the computing, then display the results on your device. Since your data is leaving your device, there's a privacy compromise. For example, if you ask for a messaging app to summarize a conversation, it may offload that computing power to a cloud server, sending the entire contents of your messages to the cloud, then back to your phone.

TEEs supposedly offer a way to keep those requests private. There are several implementations out there, like Apple's [Private Cloud Compute](#), Google's [Private AI Compute](#), and WhatsApp's [Private Processing](#). It's not just the big tech players. We've seen [chatbots](#) built with TEEs as well.

TEEs can provide more security and privacy than simply running in the clear, but they are fundamentally different from actual encryption or running locally. Despite the promises of some tech companies, they will never be able to match

that level of security and privacy. Because of that, a user's device should never automatically send data to a TEE. Let's dig through the reasons why.

What Exactly Is a TEE, Anyway?

A TEE is a hardened section of the computer that runs software in a way that's supposed to be secret even from other processes running on the machine. TEEs also let users check that the code being run is the code that they think is running, and not backdoored code instead, using a process called "attestation." You may have also heard this referred to as a "secure enclave," or heard the brand names SGX or TrustZone.

The intention of a cloud-based TEE is simple: a company can run a server in their data center, but still process data that you provide on your behalf without being able to see that information themselves.

Is a TEE Secure?

In practice, we've seen multiple cracks and hacks every year that show that it is possible to get at that data. That's because while encryption relies on math, TEEs rely on engineering to provide their security. Standard encryption algorithms are created by years-long processes collaboratively produced by mathematicians around the world and are based on problems that have been studied for decades. The math is reliable, and there is no shortcut to breaking it

that would not also upend fundamental understandings of mathematics as a field.

The collective understanding of every mathematician in the world is that standard encryption algorithms are not breakable to the best of the world's collective knowledge. No responsible engineer builds a system based on a new encryption method until after it's been offered up for prodding.

Engineering, on the other hand, doesn't work like that. Every individual system is the product of a group of engineers who put it out into the world, and each product will have its own quirks and bugs that have to be individually discovered and patched. These bugs are found after the system is built, not before. No one has yet built a system that is unbreakable. On the contrary, there is new research all the time that finds new ways to break into TEE systems. They're patched as they come up, but they're unlikely to ever become perfect, and certainly not any time soon.

TEEs in particular are a hard engineering problem because the encryption key is physically right there on the device. Building a TEE means keeping a key fully separate and inaccessible while it's on the same physical device as parts of the system that shouldn't have access to the key.

Many attacks on TEEs involve "side channels." In a side channel attack, [the attacker measures](#) the electrical impulses or other effects to figure out the timing of operations inside the TEE, then uses that to figure out the key being used. Once

they have the key, they can read all the data. Compare that to end-to-end encryption, where the key is never on that machine in the first place, so an attacker would have to also run a similar attack on the user's device.

Companies who turn to TEEs to protect data want to both have the key on the server and have it protected while still performing complex operations like running an LLM, which makes it much more difficult to protect those keys.

That being said, a TEE versus plaintext on a server is the difference between being able to easily read the data and having to do a bunch of specialized work to get at the data. That work often involves accessing the physical machine. This is most relevant for protecting against mass surveillance, and for many people, that might just be enough security.

But that's the core of the problem. "Secure enough for most cases" and "encrypted as in math" are not the same thing, and it's important not to conflate the two. And services that currently offer "encryption as in math" have a real downgrade in security when they switch to security based on TEEs.

If you want to dive into the myriad security issues and limitations of TEEs we've seen so far, they're well documented [here](#), [here](#), [here](#), and [here](#).



What Does This Have To Do With LLMs and AI?

Sometimes organizations want to offer an LLM that can respond to queries in a private manner. On-device LLMs exist, but they're limited in size. So, when organizations want to offer the ability to answer queries without being able to see the conversation, they turn to TEEs. That's a useful way to run a chatbot that's reasonably private. This is what Apple, Google, WhatsApp, and others are doing.

Why not turn to encryption? After all, LLM inference is just a bunch of math like any other things a computer does. It takes input to a (really big) function and gives an output. We have the math to do that computation in a way that hides the inputs and outputs from the one running the computation, it's just super expensive. It's called homomorphic encryption, and no one's figured out how to do it fast enough that it makes sense for this sort of computation.

Instead, the allure of a TEE is that it will run that computation for you inside of a special opaque section of a server. TEE manufacturers try to make it as hard as possible for the person running the TEE to peek inside. But you still have to trust the operator to not put a stethoscope to the box to try to figure out what's happening inside.

In this case, it's reasonable to consider these systems "privacy-preserving," but not "encrypted." That distinction is important, especially when we talk about how the TEEs

interact with secure messaging. When someone using an end-to-end encrypted chat app asks an LLM to summarize, review, or store those messages, the content of those messages is leaving the device and going to an unencrypted third-party server somewhere. That's a major threat to the privacy of secure chat apps, and one that's increasingly hard for users to take control of.

How Does This Translate to Practical Advice?

The answer to this is going to vary based on an individual's threat model, but a good rule of thumb is that a user's device should never automatically send data to a TEE. When the person holding a phone can choose what information is sent, even if it's a chunk of data like "unread messages," they have the opportunity to pause and consider if that data might be too sensitive to risk sending.

In contrast, when data is sent automatically, the automatic sending becomes a feature of the system as a whole. If the system was previously end-to-end encrypted, adding automatic exfiltration makes the whole system no longer end-to-end encrypted.

Developers: don't build systems that automatically send data off a device to a TEE, especially when it's coming from an app that is otherwise end-to-end encrypted.

Users: if developers ignore us and build that system, [turn off](#) any automatic data sending features. Take a second to think about how

much you're willing to risk sending data when you choose to send it off the device.

So, What Should I Be Concerned About?

TEEs are useful for security in a number of circumstances. Your phone likely has a TEE where it keeps the key that encrypts your biometric unlock data and the base of the keychain where passwords are stored. It also enables certain backup systems, like how you can restore a phone with your passcode or restore WhatsApp or Signal backups.

But when we're talking about cloud processing, it's important to be clear this isn't the same as end-to-end encryption and doesn't offer the same level of privacy.

Most of our private lives are on our phones and in our messages. We've worked for years to secure those messages, with major wins like encrypted RCS, and the continued user experience improvements of Signal and WhatsApp. We've even seen real improvements to backup security with features like [Advanced Data Protection](#) that bring end-to-end encryption for a variety of data outside of messaging, like notes and photos.

But as companies roll out AI features that interact with these encrypted services, pulling data off devices and into a cloud-based TEE, they're eroding the privacy protections of end-to-end encryption and risk causing serious confusion around what data is protected and what isn't.

PCLinuxOS

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

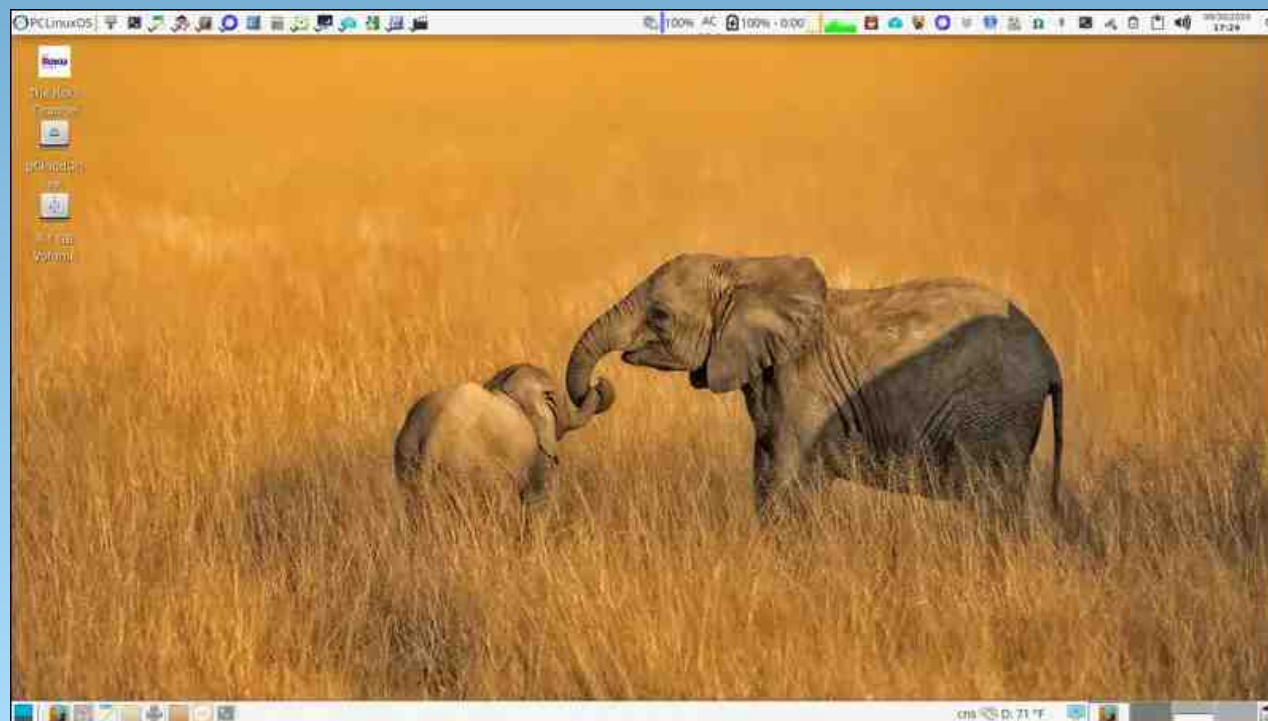
**Put Down Your
Phone & Arrive
Alive.**



PCLinuxOS Magazine Graphics Special Edition, Volumes 1 - 4

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

Screenshot Showcase



Posted by parnote, September 30, 2026, running Xfce.

Good Words, Good Deeds, Good News

compiled by Meemaw

Amazon Delivery Driver Seen Untangling, Saluting Flag



A homeowner checked her security camera and found that while a package was being delivered, her American flag was untangled, then saluted by the Amazon driver. The homeowner posted the video on social media, and it went viral.

"Thank you for reminding us that there are still people who understand what that flag represents," homeowner Angie said on Facebook". She is hoping to identify the driver so she can thank [them].

The driver was eventually identified. She didn't say she was in the military, but identified herself as a military brat.



22 Year-Old With Down Syndrome Becomes Certified Fitness Instructor



Jane & Aubry

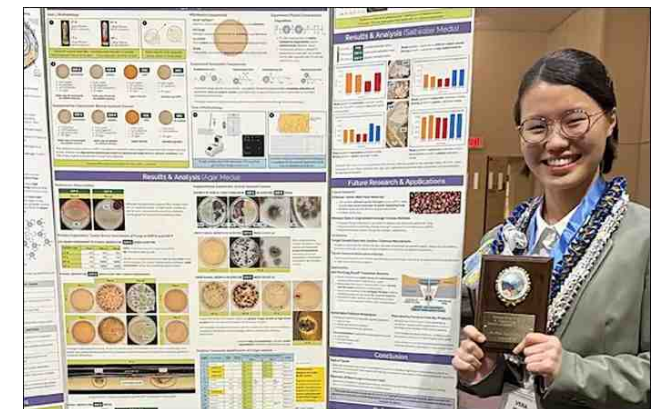
22 year-old Aubry has been certified as a fitness instructor, according to her boss, Jane, who owns VASA Fitness in Utah. Aubry is also mentally challenged, having [Down Syndrome](#).

Jane says Aubry has learned all the steps to the routines, and all the music as well. She loves to lead the workouts in the fitness center. Jane is helping Aubrey take her certification and turn it into a full-time job.

"Aubry had been attending several classes, including UpBeat Pilates, Zumba, SilverSneakers, and HIGH Fitness, but her favorite was UpBeat Barre, which according to

its website "combines strength training, Pilates, cardio, and yoga into a high-energy fusion of fun."

Hawai'i Teen Discovers Fungus That Can Filter Plastic And Sunscreen From The Sea



Vera entered the science fair with her research on fungi found in coconut husks. She found that it is successful in filtering plastic and sunscreen from the sea.

"I learned that the pore structure of coconut fiber supports the movement of air and water, which can create a favorable environment for microbes," she said. "That led me to wonder whether coconut husk could do more than physically capture pollutants. So this year, my research at the Amend Lab began exploring the fungal communities living in coconut husks and studying their growth and degradation abilities

on sunscreen and plastic media.” From that, she has shown that it can also bio-degrade those materials.

She won in multiple categories after conducting experiments in Anthony Amend’s lab at the University of Hawai‘i at Mānoa. And she qualified for the International Science & Engineering Fair taking place next May in Arizona.

After that, in genetic tests, it was also found that the fungi was a previously unknown species.

“This work was made possible because of Vera’s vision, and it gives me such optimism about the future of science in Hawai‘i,” said Amend, who is based in the Pacific Biosciences Research Center at School of Ocean and Earth Science and Technology (SOEST).

Montana Teen Uses Lasso To Rescue Drowning Man

Montana teen Jory, 14, is obsessed with roping and practices lassoing the roping dummy every chance he gets. During the 4th of July weekend this year, all that practice paid off, when he saved a man from drowning.

A group of four were rafting down the Yellowstone River nearby when they hit a bridge pier and fell in. Three of them got to safety, but the fourth was floating down the river clutching a cooler. Jory waded into the river and lassoed the man, and pulled him to safety.



Convincing the man to let go of the cooler, Jory got him around the arm and neck on his first try, while a bystander on scene rushed to help the young man reel him in.

Jory’s father, a veteran volunteer firefighter, said that he had called 911 as soon as he heard the screaming, and police records show that from the time of the call, it took just 3 minutes for a sheriff’s deputy to arrive. By then there was hardly anything to see.

Jory said he felt pretty good after he knew the man was out of the water and safe.

Service Dog Stayed With Missing Three Year-Old

In August, officials in Atchison County, Kansas responded to a report of a missing 3-year-old child. Luckily, the child was found quickly, with a friend guarding him.



In a social media post, authorities with the Atchison County Emergency Services said the child was found safe and was back with family members, then detailed how a special companion helped in the rescue.

“The hero is Maverick the dog, the bestest boy ever. Maverick was located with the child and had apparently stayed by the child’s side through the entire event. Maverick got all the treats and scratches responders could provide,” the post read.

“Service dogs are trained to perform specific tasks for individuals with disabilities, including physical, neurological, psychiatric, or medical conditions,” according to the Guide Dogs for the Blind [website](#), which added that the dog’s behavior must be focused, dependable, and responsive.

Many other social media posters praised Maverick.

Wiki Pick: Keep Your System In Good Order

Relevant to ALL editions of PCLinuxOS

You've downloaded PCLinuxOS Livecd ISO, along with the md5sum file, and burned it to your USB Flash Drive or CD Rom.

All your hardware works, and you install.

Everything works sweetly and you want to keep it that way.

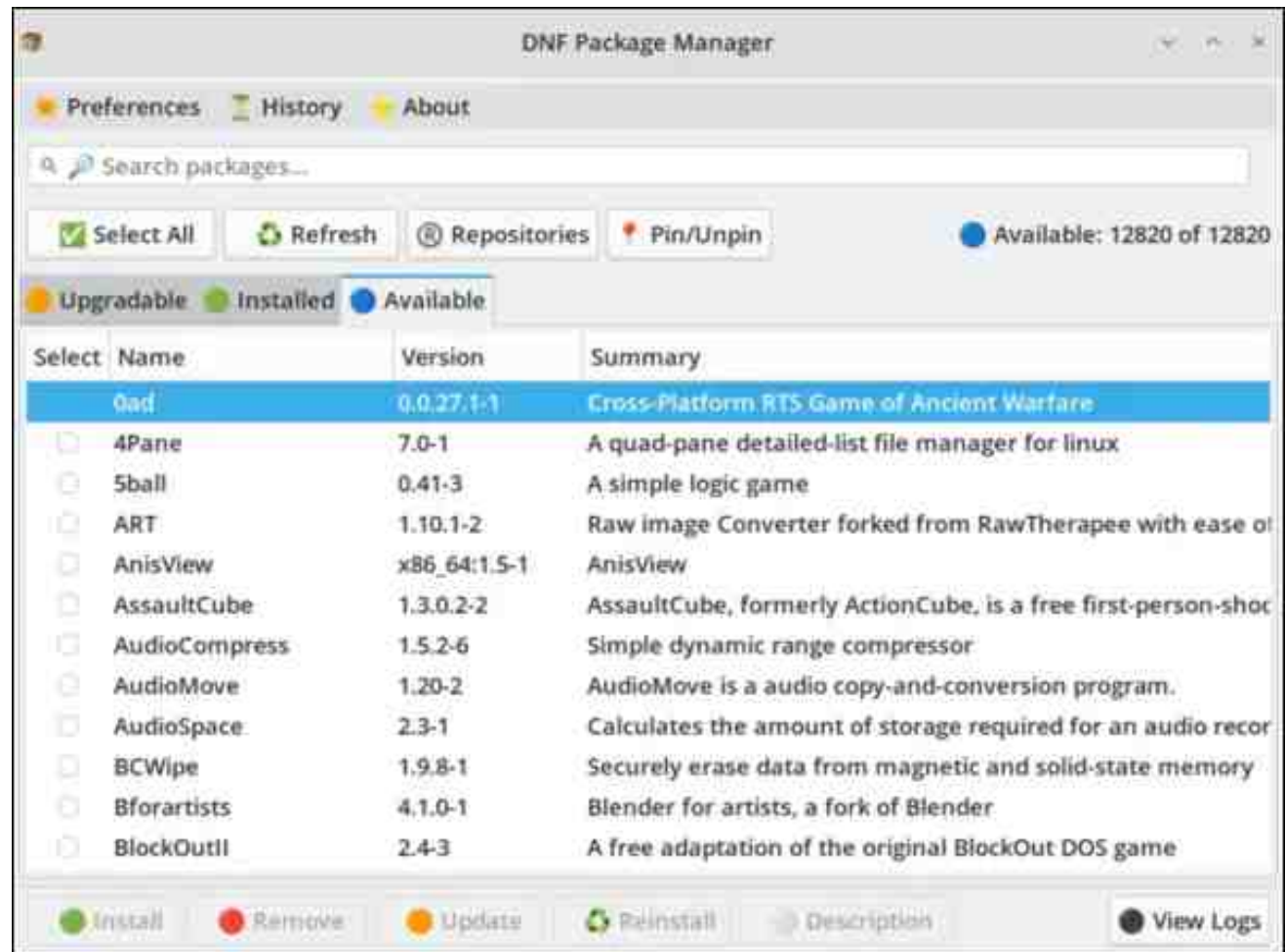
First, do a full update of the system.

(If you get a question like this, "**Some packages could not be retrieved**" - "Continue ignoring these programs ?", **'NEVER EVER** answer Yes!!! If you get this message, answer **NO** and try again later. If the problem persists check the forum for information or post a topic asking for help).

Wait for the update to completely finish.

Now you can go to your package manager and install any applications that take your fancy.

Every few days open the package manager, click **Reload** to see if there are any.



Only ever have **ONE** repository mirror enabled.. If the current mirror is sluggish, uncheck that and choose another. Click Reload afterwards to get the correct package lists from that mirror. They are all mirrors of the one central repository and don't get updated at the same time. The mirrors are in different parts of the world and

some are administered by volunteers who have to fit in maintenance with their jobs.

With more than one repo/mirror enabled, your packages list can become scrambled with incorrect entries, leading to mis-installation.

The Philosophy of PCLinuxOS

Many people ask the questions:

- * Why are packages so late arriving in the repo?
- * Why can't I install outside packages?
- * Why must I always fully update?

PCLinuxOS is a '**meta' distro,**' or '**rolling release.**' That is, it is built in such a way that the user installs and then fully updates periodically over an indefinite period, so far as much as four years, rather than fully reinstalling from the next release as with most distros.

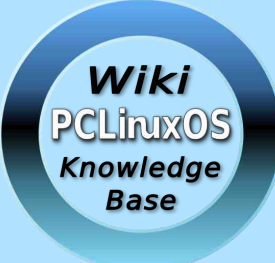
This means that a certain discipline is required of the user. The user must adhere to a program of fully updating from time to time and never installing outside packages in order to preserve the stability, thus reliability, of the system.

Packages often appear much later in PCLinuxOS than in other distros because the development and packaging teams together comprise few people and all packages are rigorously tested by them and an additional group of testers before it is permitted to grace the repo.

The strict adherence to the principles of stability has gained for PCLinuxOS a reputation for quality and usability that the developers and users are proud of, knowing that the OS is reliable for an indefinite period.

If you haven't updated your system within the past 30 days then download a fresh ISO and install from the updated CD. Updated ISOs can be downloaded from the [PCLinuxOS](#) main page.

You can access this PCLinuxOS Knowledgebase Wiki article [here](#).



**Visit.
Contribute.
Build.**

**The PCLinuxOS
Wiki**

It Belongs To YOU!

Screenshot Showcase



Posted by tbs, September 12, 2026, running KDE.

Victory! Appeals Court Rejects Expansive New Copyright Claim

by **Joe Mullin**

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons [license](#)



Image by EFF (CC-by)

The U.S. Court of Appeals for the Ninth Circuit handed internet users and programmers a big win today, by rejecting an attempt to stretch a narrow provision of the Digital Millennium Copyright Act (DMCA) into a new source of copyright liability.

The case involves Section 1202 of the DMCA, which prohibits intentionally removing copyright management information (CMI) like an author's name or a copyright notice, from a copyrighted work. Open AI and Microsoft used code from Github as part of the training data for their LLMs, along with billions of other works. A group of anonymous Github contributors sued, alleging the new code coming out of these LLMs was similar to theirs—but with the CMI stripped out.

The Ninth Circuit correctly agreed with [what we said](#) in our [brief](#): removing copyright information from a copyrighted work is fundamentally different from creating a new work that didn't have CMI in the first place. Section 1202 of the Digital Millennium Copyright Act was intended to serve as a backstop for traditional copyrights in the digital age—not to create a new, more expansive right to inhibit otherwise non-infringing uses.

As we also explained, accepting the Does' theory would have created a brand-new source of liability for otherwise perfectly lawful activities, undermining creativity and innovation far beyond the specific context of AI development. Copyright holders would be able to file costly lawsuits against all kinds of legitimate users, such as artists making remixes based on older works, teachers adapting works for a classroom presentation, engineers reverse engineering code to understand it better, and search engines that help us all navigate the web. The risks would have fallen especially hard on independent software developers and other small creators. Large companies can afford to litigate these claims in federal court for years, if necessary. But an independent programmer facing massive statutory damages may simply have to settle, even when their underlying use is completely lawful. That's why EFF fights to make sure courts don't expand copyright beyond what Congress authorized.

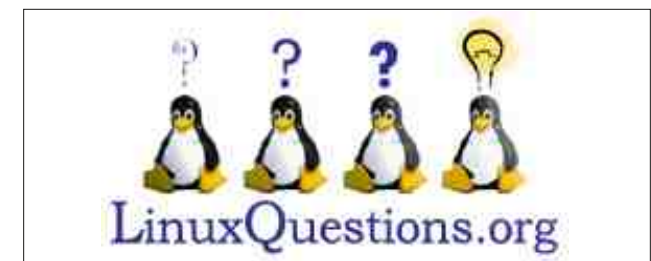
Copyright law still protects programmers when their work is unlawfully copied. They can still bring copyright infringement claims if someone uses a model to reproduce their code. Additionally, the plaintiffs' contract claims against the AI companies are still in play. The specific holding here was narrow but important: that the absence of copyright information from a new work does not mean, by itself, that someone illegally removed it.

That's the correct result. New technologies will keep raising hard questions about copyright. Courts should answer those questions by applying the rights that Congress actually authorized, not by inventing new rights that could harm expression and lawful use for everyone.

Additional Reading:

[9th Circuit Opinion](#) in Doe v. GitHub

[EFF's Amicus Brief](#) in Doe v. GitHub



PCLinuxOS Recipe Corner Bonus



Ground Beef Mummy Bread

Serves: 4

INGREDIENTS:

- 1 lb lean (at least 80%) ground beef
- 1 medium green bell pepper, cut into bite-size strips
- 1 medium red bell pepper, cut into bite-size strips
- 1 small onion, cut into thin wedges
- 1/2 cup creamy Italian dressing
- 1 loaf (1 lb) Italian bread (12 inches long), halved lengthwise
- 4 slices (6 oz) thinly sliced provolone cheese, quartered

DIRECTIONS:

Set oven control to broil. In a 12-inch nonstick skillet, cook beef, bell peppers and onion over medium-high heat 5 to 7 minutes, stirring

frequently, until beef is thoroughly cooked; drain. Stir in 1/4 cup of the dressing.

Spread remaining 1/4 cup dressing on cut sides of bread. Place both halves, cut sides up, on an ungreased large cookie sheet. Broil with tops 4 to 6 inches from heat 2 to 4 minutes or until lightly toasted. Remove bread from the broiler. Spread beef mixture on cut halves of bread. Top with cheese.

Return to broiler; broil 4 to 6 inches from heat 2 to 3 minutes or until cheese is melted. Cut each half into 2 pieces.

TIPS:

You can use any meltable cheese for these sandwiches, such as American, mozzarella or Gouda.

Italian bread has a dense texture that works well for these hot broiled sandwiches.

NUTRITION:

Calories: 760 Carbs: 67g Sodium: 1620mg
Fiber: 4g Protein: 41g



The
**PCLinuxOS
Magazine**

Created with
Scribus



PCLinuxOS Puzzled Partitions

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

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

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

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

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



SCRAPPLER RULES:

1. Follow the rules of Scrabble®. You can view them [here](#). You have seven (7) letter tiles with which to make as long of a word as you possibly can. Words are based on the English language. Non-English language words are NOT allowed.

2. Red letters are scored double points. Green letters are scored triple points.

3. Add up the score of all the letters that you used. Unused letters are not scored. For red or green letters, apply the multiplier when tallying up your score. Next, apply any additional scoring multipliers, such as double or triple word score.

4. An additional 50 points is added for using all seven (7) of your tiles in a set to make your word. You will not necessarily be able to use all seven (7) of the letters in your set to form a "legal" word.

5. In case you are having difficulty seeing the point value on the letter tiles, here is a list of how they are scored:

0 points: 2 blank tiles

1 point: E, A, I, O, N, R, T, L, S, U

2 points: D, G

3 points: B, C, M, P

4 points: F, H, V, W, Y

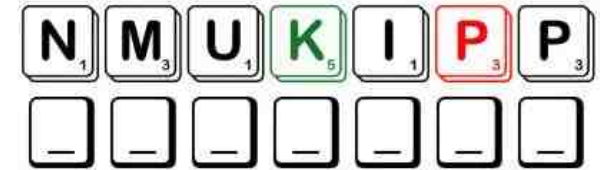
5 points: K

8 points: J, X

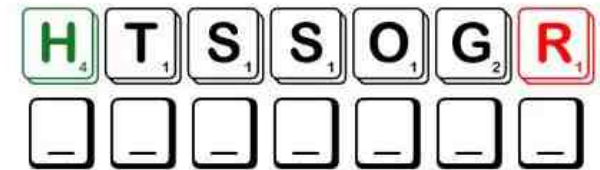
10 points: Q, Z

6. Optionally, a time limit of 60 minutes should apply to the game, averaging to 12 minutes per letter tile set.

7. Have fun! It's only a game!



Triple Word



Double Word



Possible score 263, average score 184.

Download Puzzle Solutions Here

October 2026 Word Find

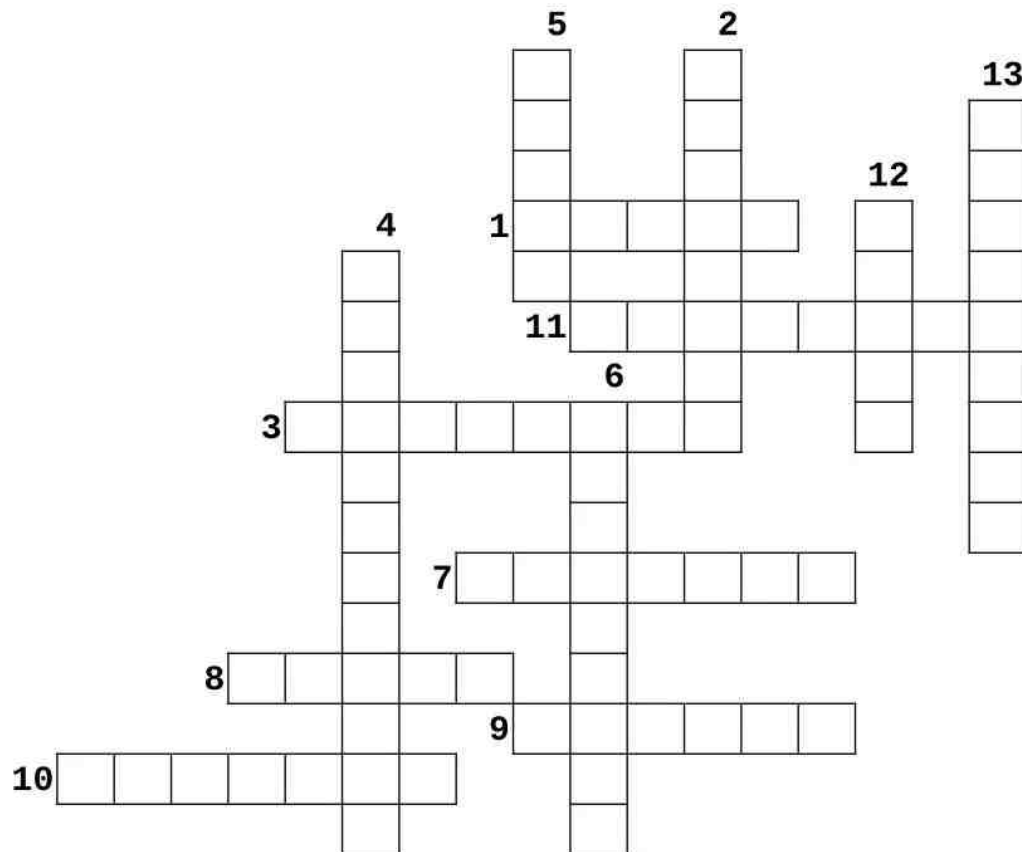
Halloween Decorations

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

ANIMATED CREATURES	BATS
BLACK CATS	CARVED PUMPKINS
CAULDRONS	CEMETERY GATES
COBWEBS	COFFIN DECORATIONS
CREEPY DOLLS	CRYPTS
DANGLING SPIDERS	EERIE FOG
EYEBALL DECORATIONS	GARGOYLES
GHOSTS	GRAVESTONES
HAUNTED HOUSES	JACKOLANTERNS
MASKS	MUMMIES
SCARECROWS	SKELETONS
SKULL CANDLES	SNAKE PROPS
SOUND EFFECTS	SPIDERS
TOMBSTONES	VAMPIRES
WITCHES	ZOMBIES

[Download Puzzle Solutions Here](#)

October 2026 Crossword Halloween Decorations



1. The physical skeletal structure of the head.
2. A heavy, round pot (often cast iron) supported over a fire.
3. The hard framework of bones or cartilage that supports an animal or human body.
4. A hollowed-out pumpkin or root vegetable carved with a face and lit with a candle inside.
5. The spirit of a dead person imagined as visiting the living.
6. A cut stone with writing on it that marks where a dead person is buried.
7. Old, messy, and abandoned webs found in undisturbed indoor areas.
8. A person—traditionally a woman—believed to have magical powers or who practices witchcraft, magic, and sorcery.
9. A dead body brought back to life by magic, science, or a virus.
10. The reanimated body of a dead person believed to come from the grave at night and suck the blood of people.
11. A grotesquely carved figure of a human or animal.
12. A stone chamber or vault, beneath the church floor, that serves as an underground burial place.
13. A model of a person dressed in old clothes and put in a field of growing crops to frighten birds away.

[Download Puzzle Solutions Here](#)

Mixed-Up-Meme Scrambler



Enjoyed at the Paris eatery ...

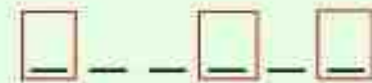
VOARP



NEFIT



COSHUR



THALLE



"

"

[Download Puzzle Solutions Here](#)

Inspiration & Motivation



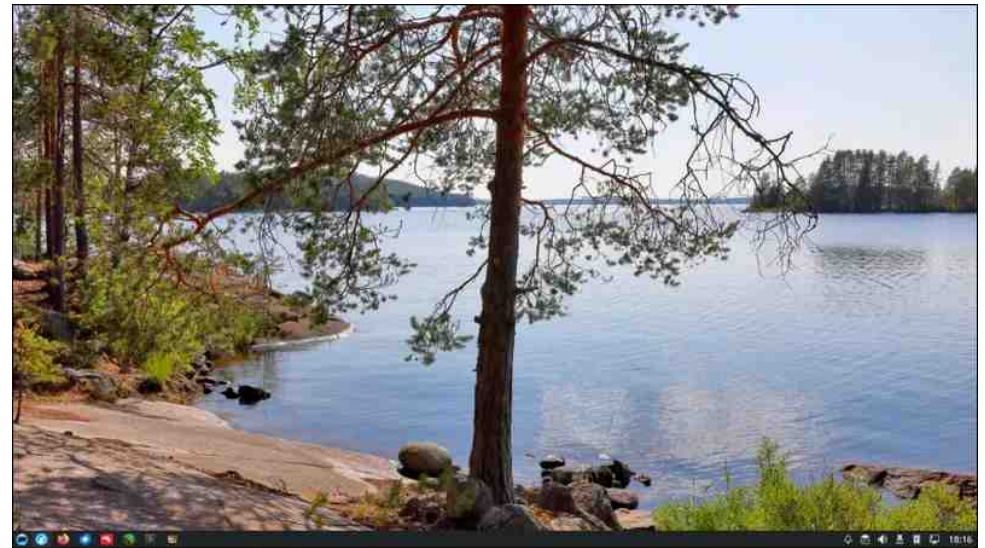
Image by Alexas_Fotos from Pixabay

***If You're Still
Looking For
That One
Person Who
Can Change
Your Life,
Take A Look
In The Mirror.***

More Screenshot Showcase



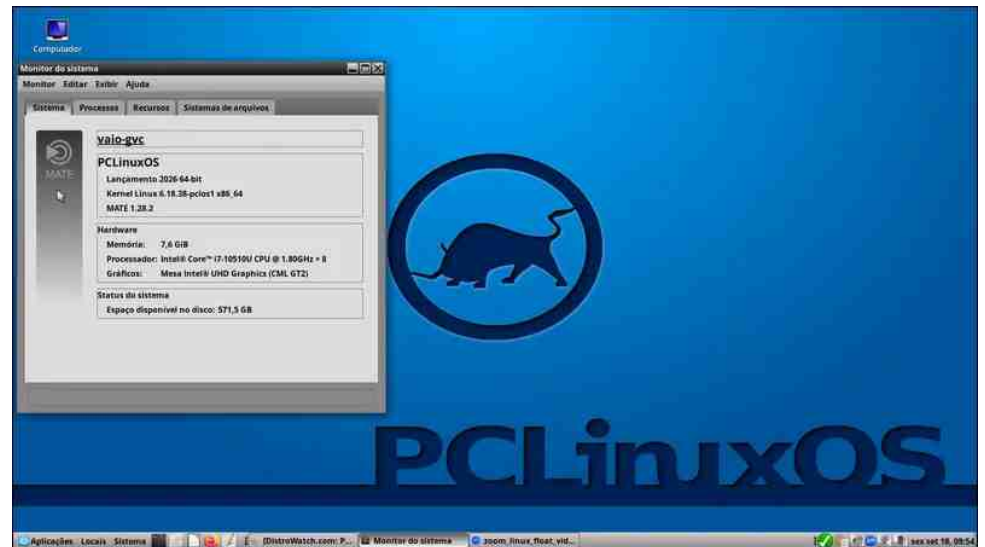
Posted by francescoinblack, September 5, 2026, running IceWM.



Posted by luikki, September 4, 2026, running KDE.



Posted by youcantoo, September 7, 2026, running KDE.



Posted by Gonzalo_VC, September 29, 2026, running Mate.