

# The PCLinuxOS magazine

Volume 180

January, 2022



Happy New Year!



# In This Issue...

- 3 From The Chief Editor's Desk...**
- 4 IDAD 2021: Counteracting Disney+'s Attack On Culture**
- 5 Screenshot Showcase**
- 6 What Google Found To Be Important To Us In 2021**
- 8 Screenshot Showcase**
- 9 PCLinuxOS Recipe Corner: Taco Stuffed Avocados**
- 10 Newspapers vs Big Tech: Antitrust Tackles The Problems  
That Copyright Just Can't Fix**
- 11 Screenshot Showcase**
- 13 GIMP Tutorial: Create A Rubber Stamp Text Effect**
- 15 Short Topix: Is The \$399 PinePhone Pro Linux Smartphone  
Enough To Gain Traction In Mobile Market?**
- 19 Chrome Users Beware: Manifest V3 Is Deceitful & Threatening**
- 20 Screenshot Showcase**
- 21 Log4J - What is the most severe vulnerability of 2021?**
- 22 Screenshot Showcase**
- 23 PCLinuxOS Bonus Recipe Corner:  
Beef and Scalloped Potatoes Casserole**
- 24 U.K. Proposal To 'Bcc' Law Enforcement On Messaging Apps  
Threatens Global Privacy**
- 25 Screenshot Showcase**
- 26 PCLinuxOS Puzzled Partitions**
- 30 More Screenshot Showcase**

## The PCLinuxOS magazine

The PCLinuxOS name, logo and colors are the trademark of Texstar.

The PCLinuxOS Magazine is a monthly online publication containing PCLinuxOS-related materials. It is published primarily for members of the PCLinuxOS community. The magazine staff is comprised of volunteers from the PCLinuxOS community.

Visit us online at <http://www.pclosmag.com>

This release was made possible by the following volunteers:

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

**Assistant Editor:** Meemaw

**Artwork:** ms\_meme, Meemaw

**Magazine Layout:** Paul Arnote, Meemaw, ms\_meme

**HTML Layout:** YouCanToo

### Staff:

ms\_meme

Meemaw

Gary L. Ratliff, Sr.

Daniel Meiß-Wilhelm

daiashi

Cg\_Boy

YouCanToo

Pete Kelly

Smileeb

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 © 2020.



# From The Chief Editor's Desk...

One thing that my eight-year-old son asked for from Santa Claus for Christmas was a computer. When he told his mom, he acknowledged that he knew they were expensive, so he wasn't really sure he would get such an expensive gift from Santa. All he knew is that he wanted it.

The "why" he wanted it is actually quite simple. First of all, he could have his own computer, just like dad's. Second, my son LOVES playing Minecraft. He's a Minecraft fiend. He plays Minecraft on his tablet. He plays a Minecraft-clone game on "his phone" (you know, my old Pixel 3 that I talked about last month).

He was absolutely convinced that the ONLY way for him to play the new Minecraft update, Caves & Cliffs, was to have a computer. We found out that wasn't really the case, but he remained steadfast in his desire for a computer.

He uses a computer at school, and is a lot more proficient with it than I realized. At school, they have the use of Google Chromebooks. Since him getting a computer was so he could play Minecraft Caves & Cliffs, getting him a Chromebook was out of the question. My brief investigation of them showed a lot of frustration on the behalf of numerous Minecrafters getting Minecraft to play on a Chromebook. So asking Santa to bring a Chromebook was pretty much a no-go proposition. It had to be a full-blown computer. And you know that typically means a computer preloaded with Windows 10 or 11. GULP!

Santa gave us a good deal on a Lenovo laptop with an Intel i5 processor, 8 GB RAM, and a 256 GB SSD. Of course, it came preloaded with Windows 10. Now seeing how dad hasn't run Windows (as an administrator, anyways) since Windows Vista came out (that's what pushed me to switch to Linux), I was



a bit "out of the loop" on setting it up. You would have laughed if you watched me and mom struggling to activate and tweak the copy of Windows 10 that came on the laptop. We were definitely floundering like a fish out of water.

If I had my druthers, Windows would be wiped and replaced by PCLinuxOS. However, I've not been able to get Minecraft to run reliably on any of my PCLinuxOS computers (and, admittedly, part of the problem may be that I really don't know my way around Minecraft ... I'm not a gamer). I definitely did not want my son to experience the same frustrations, so Windows 10 has remained on the new laptop.

We got Santa's laptop setup for my son ... eventually. One of the first things we had to do was to install Minecraft. Even that wasn't as straightforward as you might expect, since he already had a Minecraft account on his tablet. We wanted to be able to link the accounts. Aye, aye, aye! What a needlessly complicated process!

In the end, Ryan was exceptionally happy when he awoke on Christmas morning and saw that Santa had, indeed, brought him a computer. In the ensuing days, he has spent hours immersed in his Minecraft world. There's little else that beats the happiness and excitement of a child getting what he/she had wanted on Christmas morning.

Until next month, we bid you peace, happiness, serenity, prosperity, and continued good health. Be careful out there!



# IDAD 2021: Counteracting Disney+'s Attack On Culture

by zoe

Reprinted from FSF's [Defective by Design Blog](#)  
Under a Creative Commons Share-Alike license



Our fifteenth annual [International Day Against DRM \(IDAD\)](#) (held on December 10, 2021), might be over, but the fight against [Digital Restrictions Management \(DRM\)](#) continues. Each year, the Free Software Foundation (FSF) and its [Defective by Design campaign](#) distill what we've learned throughout the year in our anti-DRM activism on one "special" day: a day especially supportive to those retailers and publishers who rightly refuse to foist DRM on their customers, and a day especially critical of those who haven't gotten the message that our real digital rights cannot be restricted. For those of us steeped in the Defective by Design campaign, IDAD never fails to provide moments that inspire us in our work for the coming year.

This year, those moments came in the form of reviews that activists around the world left for Disney+ following [our call](#) to help educate those who are about to subscribe to the platform on what they *really* need to know about Disney+: not its alleged features, not the films or television shows it might have, but the way it infringes on their rights by its use of DRM. We couldn't agree more with one reviewer, who said that they wanted to be "treat[ed] as a valued client and not as a revenue source to be exploited."

We hope that this review, and others like it, are helping people to see the true "value" of Disney+.



No matter what or how many film classics it's offering, nothing can justify the unjust restriction of their subscribers. For those who've never heard the term "DRM" or thought of digital restriction before, we hope it sparked a curiosity to find out more, and start them on the path to anti-DRM activism. At the same time, we hope that the reviews also provided people who already do know something about DRM with the resolve necessary to forego it entirely and live [DRM-free](#). Reading the variety of messages different members of the community shared with

Disney+ and the Defective by Design campaign has been an invigorating experience, and as always, it's shown the dedication of the wider anti-DRM community, beginning with our community [IDAD planning meeting](#) and continuing through the Day Against DRM itself.

We've written [previously](#) about Disney+'s distinctive position among other streaming platforms. Few are sponsored by corporations with such enormous amounts of capital, and few have grown in as short



of a time as Disney+ has. Considering its vast resources (and the amount of legal know-how it's taken to unfairly [extend copyright for decades](#)), Disney+ is in a position to provide a positive example to other streaming platforms and resolve to end their practice of shackling users to their "service" by means of DRM. Instead, and like other large streaming providers such as Netflix, they fall back on the bogus excuse of "[copyright infringement](#)," something that we've long known DRM does not help prevent. That reason could also never justify the measures taken, which involve taking rights away from users and making them agree to give up control of their computers in order to have access to culture and education. Yet until they do heed the wake-up call, the Defective by Design campaign and the worldwide community of anti-DRM activists will be there to let them know that no use of DRM is acceptable.

Our [associate membership program](#) is what has helped us educate the world about the harms of digital restriction and the value of digital autonomy for years. It's also what's helped us to stage the International Day Against DRM, and powers all of the FSF's other activism. [Join](#) this effort as an FSF associate member, or [donate](#) to the campaign. It will enable us to continue to create new resources, and help carry our work against DRM into the future.

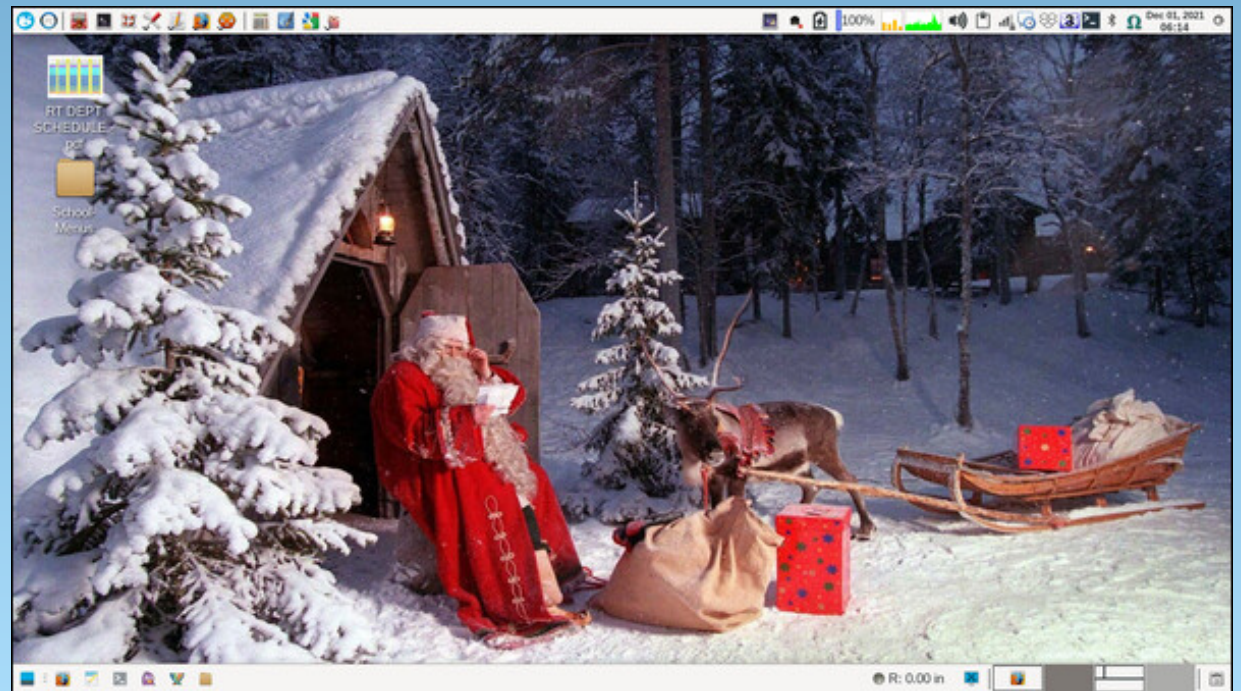
The more members we can count, the better we can help work for a world free of digital restriction. This starts with achieving our fall goal of [500 new members](#) this year-end. Associate members can select a special gift during this fundraiser, and enjoy all the [member benefits](#), which include merchandise discounts, a 16GB bootable membership card, and use of our videoconferencing server.

IDAD may be over, but our work against DRM continues. We invite you to join us in campaigning against DRM in whatever ways that interests you, whether that's suggesting edits and making corrections to the [Guide to DRM-free Living](#), joining our strategy discussions in the [#dbd IRC channel](#),

spreading the message about the Defective by Design campaign far and wide through the use of our [printable](#) resources, and by continuing to speak out for your rights wherever you can. It's certainly not too late to leave Disney+ a well-worded review! In fact, we hope you'll continue posting reviews like this one on all DRM providers' apps, and that you'll let us know if any of your reviews are ever censored. We have to work together to hold these companies more accountable.

If anything's become clear in the fifteen years we've been leading the Day Against DRM, it's the value of what a dedicated group of activists can accomplish. Sometimes, that "value" is warning about how corporations impose digital restrictions, and sometimes it's letting DRM-free publishers and storefronts know that you value their respect for digital autonomy. Each and every thing we can do to whittle away DRM's influence has real importance, and contributes to a future where a piece of media doesn't have to come at the cost of your freedom.

## Screenshot Showcase



*Posted by parnote, on December 1, 2021, running Xfce.*

# What Google Found To Be Important To Us In 2021



by Paul Arnote (parnote)

By now, everyone knows that Google collects every little scrap of data that it can grab hold of. So, it should be no surprise that Google has come out with the top 10 search terms across a dozen different categories that people searched for on Google.

I know ... I know. There are many who don't use Google any more ... or any more than they have to. And, it's not without a valid reason. Google, having long ago departed from their "do no evil" mantra, has eroded the trust that the public and users had put in them. But, you can also make a sane argument that if these were the most popular search terms on Google, then the search terms were probably similar

on other search engines that do more to protect user privacy, like StartX and DuckDuckGo.

If nothing else, Google's search results rankings help delineate the topics that we most cared about during 2021. Across much of the world, COVID restrictions and lockdowns were relaxed, and people sought to start to get back to life as they remembered it.

The dozen categories that Google lists are:

- Searches
- News
- Actors
- Athletes
- Foods
- Games
- Movies
- Passings
- People
- Songs
- Sports Teams
- TV Shows

These 12 areas are listed, by default, in their global rankings. You can, on the Google Trends site, look at the search results unique to your country. After all, I doubt users in Thailand care as much about baseball as users in the United States. Just click on the spinner next to the word "Global" on the trends site, and select the country you want to see the search results rankings for. Go ahead. You will likely be surprised at how different the search result rankings are for your area, compared to the global numbers.

So, here are the top 10 searches for each category, under the global results.



## Searches

1. Australia vs India
2. India vs England
3. IPL
4. NBA
5. Euro 2021
6. Copa América
7. India vs New Zealand
8. T20 World Cup
9. Squid Game
10. DMX

## News

1. Afghanistan
2. AMC Stock
3. COVID Vaccine
4. Dogecoin
5. GME Stock
6. Stimulus Check
7. Georgia Senate Race
8. Hurricane Ida
9. COVID
10. Ethereum Price

## Actors

1. Alec Baldwin
2. Pete Davidson
3. Aryan Khan
4. Gina Carano
5. Armie Hammer
6. Carmen Salinas
7. Shehnaaz Gill
8. Elliot Page
9. Dave Chappelle
10. Brenda Song

## Athletes

1. Christian Eriksen
2. Tiger Woods
3. Simone Biles
4. Emma Raducanu

5. Henry Ruggs III
6. Neeraj Chopra
7. Shohei Ohtani
8. Odell Beckham Jr.
9. Rafael Nadal
10. Tyson Fury

## Foods

1. Birria tacos
2. Nasi goreng
3. Feta pasta
4. Charcuterie board
5. Shōgayaki
6. Potato Soup
7. Teriyaki Amberjack
8. Tonjiru
9. Baked oats
10. Overnight oats

## Games

1. PopCat
2. FIFA 22
3. Battlefield 2042
4. Monster Hunter Rise
5. Resident Evil Village
6. Genshin Impact
7. Call of Duty: Vanguard
8. Far Cry 6
9. Madden NFL 22
10. Metroid Dread

## Movies

1. Eternals
2. Black Widow
3. Dune
4. Shang-Chi and the Legend of the Ten Rings
5. Red Notice
6. Mortal Kombat
7. Cruella
8. Halloween Kills
9. Godzilla vs. Kong
10. Army of the Dead

## Passings

1. DMX
2. Gabby Petito
3. Marília Mendonça
4. Prince Philip
5. Brian Laundrie
6. MC Kevin
7. Lázaro Barbosa de Sousa
8. Peter R. de Vries
9. Paulo Gustavo
10. Helen McCrory

## People

1. Alec Baldwin
2. Kyle Rittenhouse
3. Christian Eriksen
4. Tiger Woods
5. Simone Biles
6. Joe Biden
7. Emma Raducanu
8. Derek Chauvin
9. Henry Ruggs III
10. Pete Davidson

## Songs

1. drivers license, Olivia Rodrigo
2. MONTERO (Call Me by Your Name), Lil Nas X
3. INDUSTRY BABY, Lil Nas X feat. Jack Harlow
4. Fancy Like, Walker Hayes
5. MAPA, SB19
6. good 4 u, Olivia Rodrigo
7. Butter, BTS
8. Jalebi Baby, Teshar
9. Wellerman, Nathan Evans
10. Good Days, SZA

## Sports Teams

1. Real Madrid CF
2. Chelsea F.C.
3. Paris Saint-Germain F.C.
4. FC Barcelona

5. Sociedade Esportiva Palmeiras
6. Los Angeles Lakers
7. Sport Club Corinthians Paulista
8. Boston Red Sox
9. São Paulo FC
10. Manchester City F.C.

## TV Shows

1. Squid Game
2. Bridgerton
3. WandaVision
4. Cobra Kai
5. Loki
6. Sweet Tooth
7. Lupin
8. Ginny and Georgia
9. True Beauty
10. BBB21

Admittedly, there are things on this list that I've NEVER heard of (or wondered about) before. Your "surprise" is likely to be as strong as mine.



## Screenshot Showcase



*Posted by tuxlink, on December 6, 2021, running KDE.*



# PCLinuxOS Recipe Corner



## Taco Stuffed Avocados

Serves 4

### INGREDIENTS:

1 tablespoon avocado oil  
8 ounces lean ground turkey  
¼ cup chopped onion  
1 teaspoon chili powder  
¼ teaspoon salt  
½ cup low-sodium black beans, rinsed  
¼ cup salsa  
2 ripe avocados, halved and pitted  
1 tablespoon chopped fresh cilantro  
1 teaspoon lime juice  
4 teaspoons shredded Mexican cheese blend

### DIRECTIONS:

1. Heat oil in a medium skillet over medium-high heat. Add ground turkey, onion, chili powder and salt. Cook, stirring with a wooden spoon and breaking up large pieces of turkey, until cooked through, 4 to 6 minutes. Remove from heat and stir in black beans and salsa.

2. Carve out the flesh of each avocado half with a spoon, leaving about a 1/4-inch border all around.

Transfer the scooped flesh to a small bowl. Add cilantro and lime juice; mash with a fork until chunky-smooth.

3. Fill each avocado half with about 1/2 cup of the turkey filling (they will be very full). Top each with 1 teaspoon cheese and some of the guacamole.

### NUTRITION:

Calories: 324  
Fiber: 8.9g  
Protein: 15.4g

Carbs: 15.6g  
Sodium: 754.8mg



The PCLinuxOS  
Magazine

Created with  
Scribus



# Newspapers vs Big Tech: Antitrust Tackles The Problems That Copyright Just Can't Fix

by [Cory Doctorow](#), EFF

Reprinted from Electronic Frontier Foundation  
Under a [Creative Commons Attribution License](#)



More than 200 newspapers have filed suit against Google and Facebook (AKA “Meta”), alleging that the tech giants colluded to rig ad markets so that they could misappropriate ad revenues that were properly owed to the publishers.

*Strip away all the ornamental complexity and it's obvious that the surveillance advertising industry is designed to shift value from advertisers and publishers to Big Tech*

The evidence that Google and Facebook rigged this market is strong. [Strip away all the ornamental complexity](#) and it's obvious that the foundations of the surveillance advertising industry are designed to shift value from advertisers and publishers to the tech companies that operate the “real time bidding” exchanges that process hundreds of billions in ad dollars.

The UK Competition and Markets Authority's [wide-ranging and comprehensive study of the ad-tech marketplace](#) found many ways in which these

markets were rigged to the detriment of publishers, and [unsealed documents from antitrust prosecutions in the USA](#) revealed explicit, undeniable collusion between the tech giants.

Together, Google and Facebook command 80% of the search and online display advertising market. Either one is in a position to bend that market to their advantage. Together, they are devastating, as [the newspapers' briefs show](#). How did they attain this remarkable scale?

Primarily, they bought that dominance. The tech giants - like [the industrial giants that dominate virtually every sector of the economy](#) - bought up their nascent rivals and merged with their largest competitors, until for many people, the internet was reduced to [five giant websites, filled with screenshots of text from the other four](#).

The plain language of America's antitrust laws prohibit these kinds of mergers, but for forty years, that statutory language has been ignored in favor of a weak, ineffectual “consumer welfare” standard. This standard permitted runaway mergers and acquisitions and [celebrated the market concentration that emerged from it as “efficient.”](#)

Thankfully, the tide has begun to turn against “consumer welfare.” Last summer, the Biden administration [officially announced its intention to enforce antitrust law beyond the narrow confines of consumer welfare](#). Congress [wants to end Big Tech's acquisition shopping-spree](#), which saw tech giants buying companies [more often than most of us buy groceries](#). The movement to reinvigorate antitrust law is not merely an American affair, either: the UK Competition and Markets Authority [just ordered Facebook to sell off Giphy](#), a nascent competitor that would have given Facebook the

ability to monitor users of competing, non-Facebook social media services. In Europe, [the EU Parliament's proposed Digital Markets Act seeks to curb tech's power](#) over its users, [its regulators](#), and its supply chain.

That supply chain includes the newspapers, of course.

Newspapers are right to be concerned that Facebook and Google had rigged the system and misappropriated billions that were owed to them. It's wonderful to see the press calling out market concentration as a threat to economic liberty and a source of rot and corruption within markets.

It's also a very welcome evolution of the media's longstanding position that the problem with the tech giants was [their failure to pay for the privilege of linking to newspapers](#). This is just wrong: the tech giants aren't stealing publishers' content - they're stealing publishers' *money*.

That's a distinction with a difference. Laws that make tech pay for links - like [the European Copyright Directive of 2019](#) - only strengthen Big Tech's monopoly, by pricing links out of the budget of potential competitors.

*Competition problems need to be fixed with competition law, not copyright.*

Giving newspapers a special copyright (or a new copyright-like legal tool) that lets them dictate who can utter the factual statement that “a news story exists at this URL” won't correct the power imbalance that lets a monopolized tech sector rip off publishers. Competition problems need to be fixed with competition law, not copyright.



# Newspapers vs Big Tech: Antitrust Tackles The Problems That Copyright Just Can't Fix

After all, the newspaper industry has its own competition problem. Vulture capitalists [have bought and looted hundreds of newspapers across the country](#) (and elsewhere, [including Canada](#)). A link tax lets these new finance-sector owners increase their balance sheets without actually investing in news, by shifting billions from tech monopolists' bank accounts to media monopolists' side of the ledger.

By contrast, unrigging the ad markets will provide billions to the newspapers that invest in the most important, widely read news stories. Ad markets have a competition problem, so fixing them with competition law makes sense.

Ad markets also have a [surveillance problem](#). Big Tech's addiction to spying on us and their billions of nonconsensual dossiers about our lives and preferences have distorted the ad market such that nearly all advertising today is targeted on the basis of behavior (who you are) rather than context (what you're reading).

*America is long overdue for a federal consumer privacy law with a private right of action*

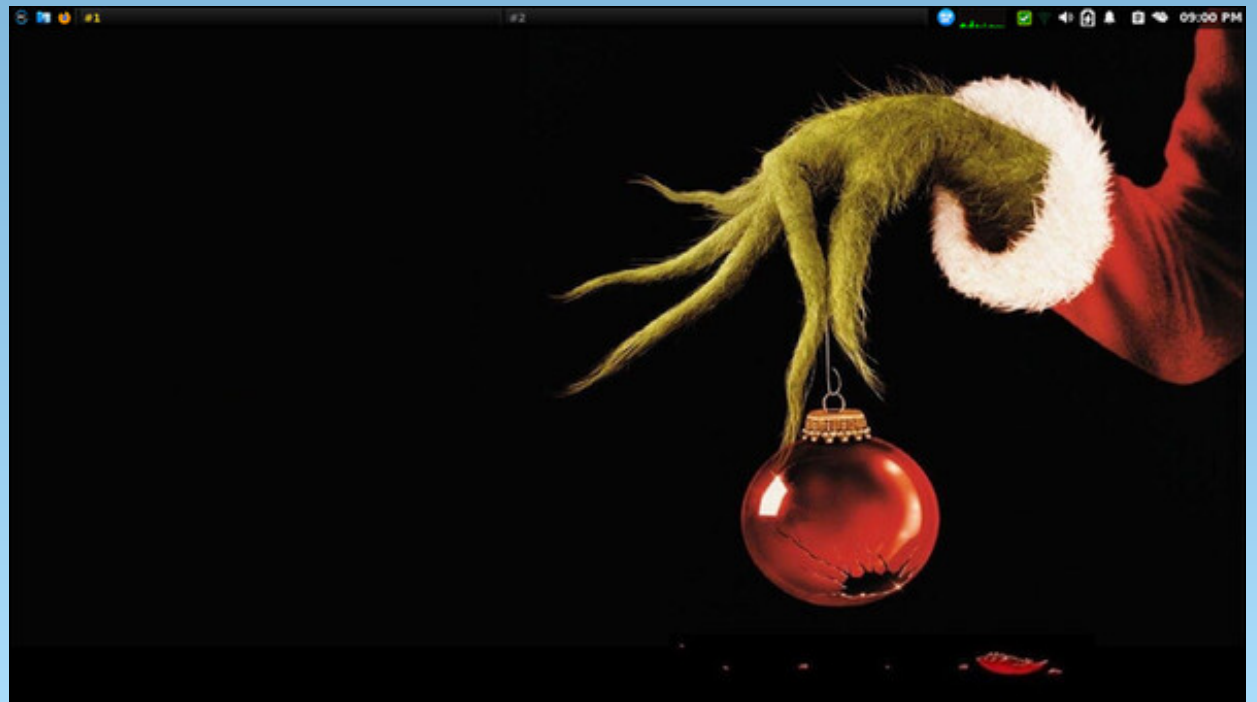
That could change: America is long overdue for a federal consumer privacy law with [a private right of action](#) (which would give you the right to sue companies that broke the law, rather than waiting for a government agency to take up your case). An ad marketplace stripped of surveillance [can thrive](#), and what's more, such a market [would especially benefit newspapers](#), whose articles are rich in the kind of context that is perfect for contextual advertising.

Ending the surveillance business model would be good for newspapers—and bad for Big Tech. Google and Facebook's vast repositories of private information currently sit on their balance sheets as assets to be monetized. Prohibiting data-processing without consent would strand those assets, [turning them into toxic waste](#).

In other words, part of the tech giants' leverage over newspapers is data, which they treat as the "new oil." A privacy law would force these companies to recognize that their data isn't a stockpile of oil - it's [a pile of oily rags](#). "Saving news" is a matter of

weakening tech's ability to misappropriate newspaper revenues, and structuring markets to reward newspaper reporting. Copyright is largely irrelevant to both of those tasks. Competition and privacy law, on the other hand, are key.

## Screenshot Showcase



*Posted by Ximru, on December 1, 2021, running Mate.*

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

**PCLinuxOS Magazine's  
searchable index!**

The **PCLinuxOS** magazine



Visit.  
Contribute.  
Build.

The PCLinuxOS  
Knowledge Base  
*It Belongs To YOU!*



JUPITER  
BROADCASTING

Podcasts For Linux & BSD



## 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. All trademarks are the property of their respective owners.
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.



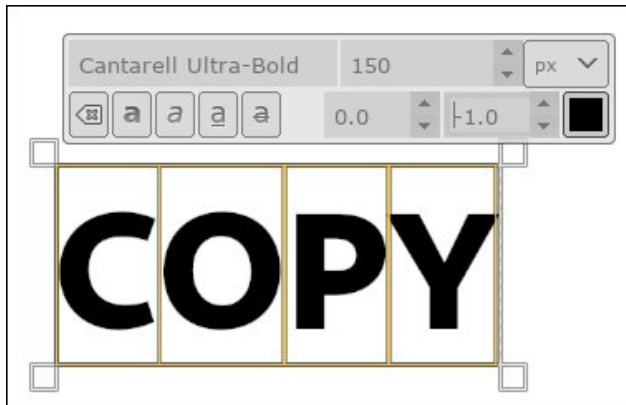


# GIMP Tutorial: Create A Rubber Stamp Text Effect

by Meemaw

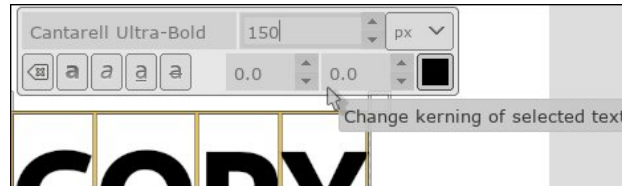
I found this as a Photoshop tutorial, and I always experiment with Photoshop tutorials to see if they work in GIMP. This one had several effects that I wasn't sure of (I've never used Photoshop), so I tailored it to GIMP.

To begin, go to the **File > New...** menu item and create a new document with a white background at the desired size and resolution.

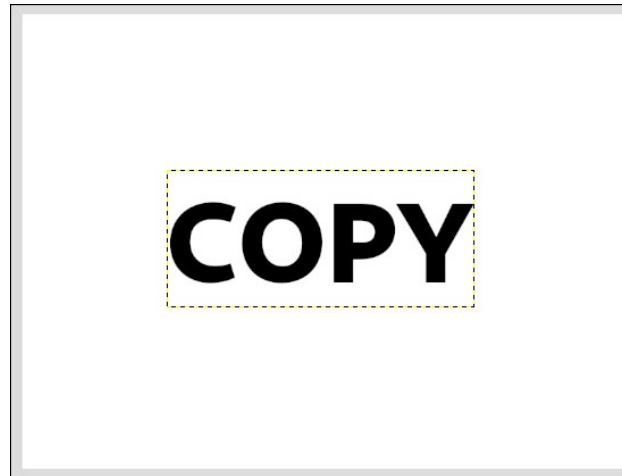


It will work better if you use a heavy font. I'm using Cantarell Ultra Bold. Make it fairly large (150 pts in this image) and type in uppercase. You can keep the color as black.

If with your font, you don't like the tight spacing between the letters, you can easily fix it through the text tool panel. You can find the kerning adjustment on the right side of the text settings (center, top).

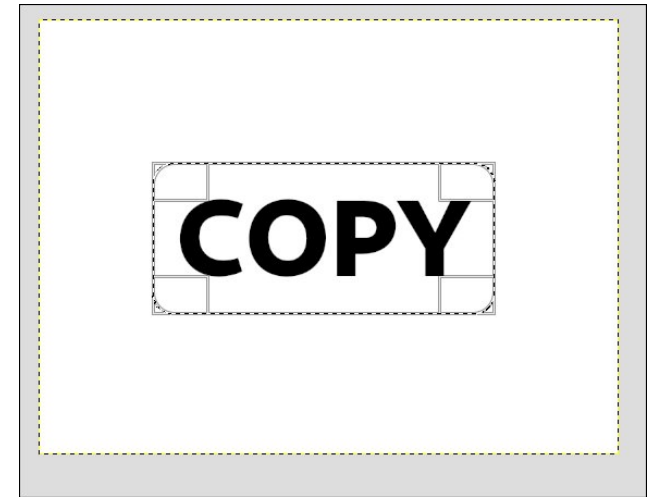


Click between the letters whose spacing you want to adjust, or select all text and then from the kerning display, set the kerning value to a larger or smaller number to increase or decrease character spacing.



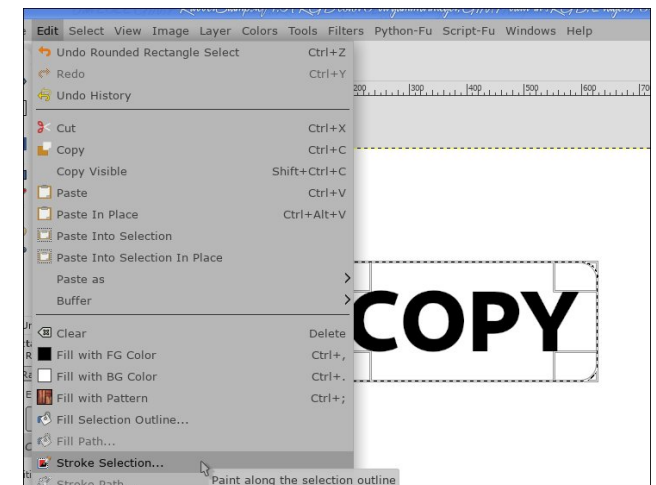
While you are adjusting, center your text on the page. If you decide you want it bigger, scale the text layer.

Now we're going to put a rounded rectangle around our text (some stamps have boxes around them). I did this on a new transparent layer rather than the text layer. Using the **Rectangle Select** tool, make sure **Rounded Corners** is chosen and make the radius 30, or whatever looks good to you (top, right).

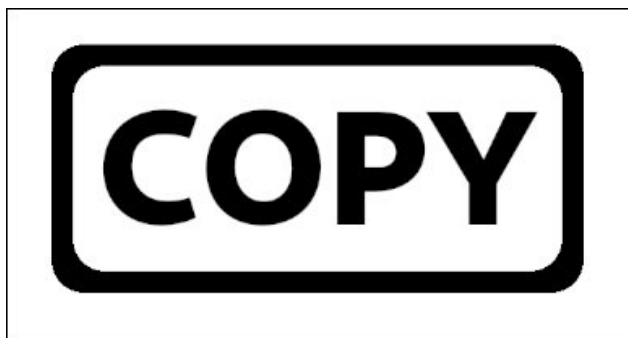


Draw the rectangle a bit larger than your text so it surrounds it with some space on all the sides.

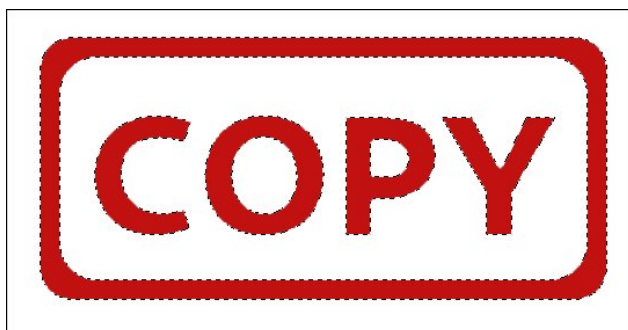
When you get your rectangle drawn, go to **Edit > Stroke Selection** to add the stroke color to the box. Make your stroke width about 20.



Make sure your rectangle is centered under your text using the Move tool. Once you have them aligned, you can merge the two layers.

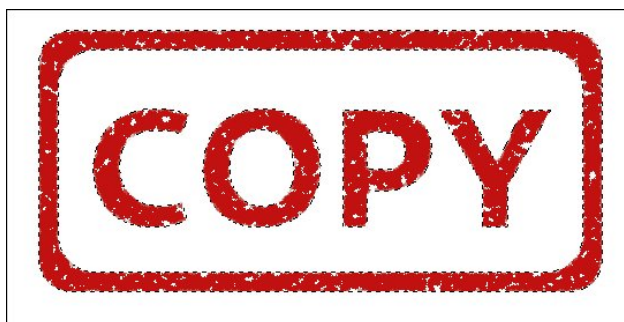


Now we need to do the pattern. Since your drawing is just black so far, choose the Select By Color tool and click on the black. GIMP should choose your text and your rectangle. If you want to change the color of your stamp, you can do it now.



With your text still selected, go to **Filters > G'MIC > Patterns > Sponge**. I made my size 7, but you should play with it to see what you like. Now it looks a bit like a rubber stamp. Since you're finished editing text, you can choose **Select > None** to deselect your text and box (center, top).

The next thing I did was to rotate the stamp just a little and crop it. Also, if you want to actually use it for a stamp, you can select the white background layer and delete it. Then you can export it as a .png



so you can add it to a document, if that's your aim. One boss I worked for kept copies of all important papers (before offices were more paper-free), and each copy he kept was stamped with a stamp that said "COPY".



So I have made a copy of this recipe, and "stamped" it "COPY". In LibreOffice, you can insert the image, with no wrap (or wrap through), and set the stamp image at 50% opacity (top, right).



## Amish Breakfast Casserole

TOTAL TIME: Prep: 15 min. Bake: 35 min. + standing  
YIELD: 12 servings +

### Ingredients

1 pound sliced bacon, diced  
1 medium sweet onion, chopped  
6 eggs, lightly beaten  
4 cups frozen shredded hash brown potatoes, thawed  
2 cups (8 ounces) shredded cheddar cheese  
1-1/2 cups (12 ounces) 4% cottage cheese  
1-1/4 cups shredded Swiss cheese

### Directions

**1.** Preheat oven to 350°. In a large skillet, cook bacon and onion over medium heat until bacon is crisp; drain. In a large bowl, combine remaining ingredients; stir in bacon mixture. Transfer to a greased 13x9-in. baking dish.  
**2.** Bake, uncovered, 35-40 minutes or until a knife inserted near the center comes out clean. Let stand 10 minutes before cutting. Yield: 12 servings.

### Nutritional Facts

1 piece: 273 calories, 18g fat (10g saturated fat), 153mg cholesterol, 477mg sodium, 8g carbohydrate (3g sugars, 1g fiber), 18g protein.

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

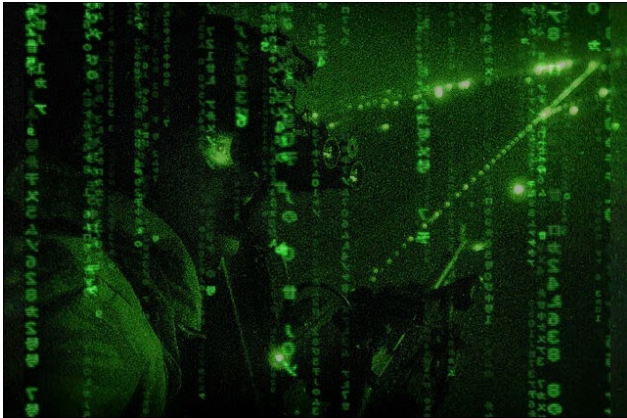
PCLinuxOS  
Radically Simple



# Short Topix: Is The \$399 PinePhone Pro Linux Smartphone Enough To Gain Traction In Mobile Market?

by Paul Arnote (parnote)

## The War On Your Privacy: Monthly Update



It's not very often that we get an ally in the fight to protect our privacy, so this bit of news is definitely welcomed. **DUCKDUCKGO, THE MAKERS OF THE INTERNET SEARCH ENGINE WITH THE SAME NAME, ARE MAKING A PRIVACY-FOCUSED DESKTOP BROWSER**, according to a [blog entry](#) by their CEO, Gabriel Weinberg. The DuckDuckGo mobile browser is THE hottest download in the Google Play store, and the second hottest download on the Apple iOS AppStore. The desktop version will function just like the mobile version of their browser.

Here's an excerpt from the aforementioned blog post:

*Like we've done on mobile, DuckDuckGo for desktop will redefine user expectations of everyday online privacy. No complicated settings, no misleading warnings, no "levels" of privacy protection – just robust privacy protection that works by default, across search, browsing,*

*email, and more. It's not a "privacy browser"; it's an everyday browsing app that respects your privacy because there's never a bad time to stop companies from spying on your search and browsing history.*

*Instead of forking Chromium or anything else, we're building our desktop app around the OS-provided rendering engines (like on mobile), allowing us to strip away a lot of the unnecessary cruft and clutter that's accumulated over the years in major browsers. With our clean and simple interface combined with the beloved Fire Button from our mobile app, DuckDuckGo for desktop will be ready to become your new everyday browsing app. Compared to Chrome, the DuckDuckGo app for desktop is cleaner, way more private, and early tests have found it significantly faster too!*

**THE GOOGLE CHROME BROWSER EXPERIENCED NOT ONE, BUT TWO SECURITY UPDATES** during the month of December, 2021. The first one was a security update of the vulnerable browser on December 5, 2021. That update addressed 20 security vulnerabilities, 16 of them reported by outside researchers, and 15 of which were rated as "high severity," according to an [article](#) on the SecurityWeek website. Then, on December 13, 2021, Google patched the desktop browser AGAIN to address five security flaws. One of those vulnerabilities was a high-risk zero-day vulnerability that was already being exploited "in the wild" by hackers, according to an [article](#) on the Tom's Guide website. Seems to validate one line of thinking that the more complex you make the browsers, the more vulnerable they are.

**2021 WAS A BANNER YEAR ... FOR PASSWORD VULNERABILITIES.** It seems the message just isn't getting through – or isn't being heeded – about not reusing passwords between sites, and using unique passwords for every site you visit. An [article](#) on

TechRepublic lists the top 10 password snafus that occurred in 2021, according to Dashlane's sixth annual list of the year's worst password offenders. Most of the "snafus" occurred because of stolen or hacked passwords.

**A GOOGLE PLAY APP WITH OVER 500,000 DOWNLOADS WAS FOUND TO BE SENDING USERS' CONTACT LISTS TO A SERVER IN RUSSIA**, according to an [article](#) on ArsTechnica. The app, called "Color Message," is infected with the Joker malware, and sends a user's contacts to a server located in Russia. Furthermore, the malware also signs users up for often-expensive subscriptions. To hide, the application can hide its icon, making it difficult to detect and remove. The Joker malware "simulates clicks and intercepts text messages in an attempt to surreptitiously subscribe users to paid premium services they never intended to buy. Joker is hard to detect because of the tiny footprint of its code and the techniques its developers use to stash it. Over the past few years, the malware has been found lurking in hundreds of apps downloaded by millions of people," according to the ArsTechnica article. Although the app has been removed by Google from the Google Play store, users who might have installed the app should remove it from their devices as soon as possible.



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

Follow PCLinuxOS on Twitter!

<http://twitter.com/iluvpclinuxos>

## Short Topix: Is The \$399 PinePhone Pro Linux Smartphone Enough To Gain Traction In Mobile Market?

### Grinch-Bots Play Grinch For Christmas



Didn't get (or buy) what you wanted for Christmas? You might have been "squeezed out" of the chance

to buy a popular gift or gift card by "Grinch Bots" that scoop up limited supplies of popular gifts, according to an [article](#) on TechRepublic. The thing is, these automated all-in-one bots work overtime (no breaks needed) to steal gift cards and buy up popular gift items so they can be resold at grossly marked up prices. [According](#) to the Kasada Threat Intelligence Team, who discovered the bot activity, the bots mimic human activity in an effort to skirt anti-bot code that's executed on the client side of public devices.

While most bot activity originates from China, during the five day period from Thanksgiving through Cyber Monday, that was not the case. Instead, over 42% of bot activity during that time frame originated in the U.S., with Australia taking second place with over 27% of the bot activity, and the U.K. coming in a distant third place with over 4% of the bot activity.

The increased bot activity included a four-fold increase in automated gift card cracking attempts, along with a ten-fold increase in malicious login attempts. It sounds like the name "Grinch Bots" is an accurate one, and one that circumvented anti-bot code on ecommerce sites. Bot activity went from nearly 0% just before "hype sales" (where a limited stock of an item is listed at a deeply discounted price starting at a specific time), to over 99% of the recorded traffic until the item was sold out. The pattern would repeat during the five day period for every "hype sale" whenever a new item was offered.

### Will \$399 PinePhone Pro Explorer Edition Linux Smartphone Finally Allow Linux Smartphones To Gain Traction In Mobile Market?

To answer the question, maybe or maybe not. The mid-range \$399 smartphone is expected to be available in early January. The phone is designed to be hackable, and comes with Manjaro Linux and KDE Plasma Mobile interface, according to an [article](#) on the Liliputing website. Sporting a microSD card slot, other operating systems – even other Linux



mobile operating systems – can be installed in Manjaro's place, and even booted from the microSD card slot. It has a 3,000 mAh battery, and a headset jack, in addition to the microSD card slot. To facilitate privacy, included phone hardware such as the camera, wifi, mic and headphone jack can be disabled with physical switches, if so desired.

So why might this attempt NOT catapult Linux smartphones into the mainstream? First of all, the name is unwieldy and long. Most of the "successful" entries into the smartphone market have short, easy to remember and say names, like "Pixel," "iPhone," and "Nexus." With a name like "PinePhone Pro Explorer Edition Linux Smartphone," it's a mouthful.

Secondly, it currently supports 4G LTE, but not the ever-expanding 5G networks that are becoming more plentiful by the month, if not by the day. That alone should limit the new phone's appeal to a large part of the mobile market. I can't imagine paying \$400 for a phone loaded with old technology, and I suspect a lot of other users might feel the same. It will definitely limit its usefulness over the long term. Who wants to be left holding \$400 worth of silicon, plastic and glass that can't connect to anything (as cellular technology evolves, 4G LTE networks will go



## Short Topix: Is The \$399 PinePhone Pro Linux Smartphone Enough To Gain Traction In Mobile Market?

the way of 2G and 3G networks) or offer access to more robust services?

And third and finally, by not being attached to a major cellular carrier, only the diehard phone users are going to be using this device. Many people, when they sign up for service, usually opt for one of the phones offered by the cellular carrier. They are guaranteed those phones will work with that carrier's network without major hassles and technical hoops to jump through, and they can get those phones without having to plunk down large sums of cash to buy the phone outright. For the latter, most cellular carriers will allow users to pay for their phone purchase over many months (usually the length of the contract), making more expensive, higher-end phones accessible for those who cannot pay those often really high prices.

### The "Why We're Glad We Don't Run Windows" Department



When Windows 11 came out, **Microsoft had made it next to impossible to use any other web browser** other than Microsoft Edge. It was possible,

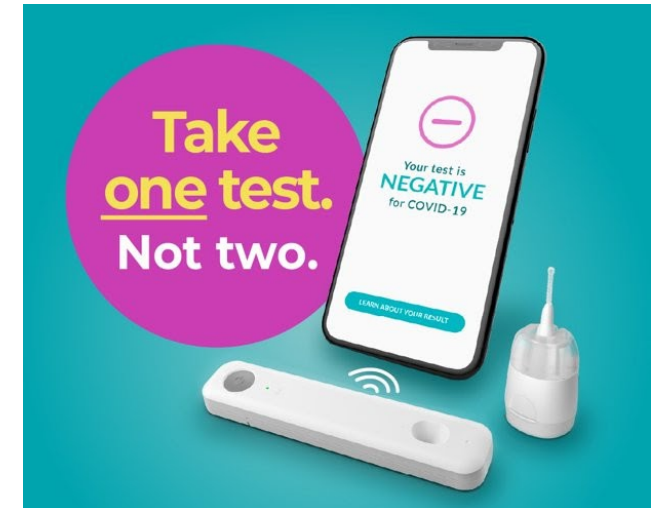
but it was a difficult path that most users just couldn't or wouldn't follow, fraught with minefields and pitfalls at every twist and turn. Well, according to an [article](#) on the Verge website, Microsoft has backed off from trying to ram Edge down everyone's throat, and has made switching browsers a one-click affair.

Most of us around here have, at one time or another in our previous computing life, been a Microsoft Windows user. One thing that has hardly changed since the birth of Windows is the default text editor in Windows, called Notepad. According to an [article](#) on the ArsTechnica website, **Microsoft has finally given Notepad an update with Windows 11**. The updated text editor allows users to change between a light and dark mode, and sports more modernized font controls. Under the hood, it features a new find and replace dialog box, as well as a multilevel undo function.

It appears that **Windows 11 is responsible for cutting the performance of NVMe drives by approximately half** for many users of the new operating system, according to an [article](#) on the digitaltrends website. Many reports of essentially the same behavior have flooded Reddit forums in recent months. While Microsoft hasn't taken an official stance or released an official reply, one Microsoft employee replied on one of the Reddit threads that the Microsoft file systems team is investigating the issue.



### Oooops! Home Covid Test Susceptible To Hacking



Widely reported on in both the computer press and the mainstream media, the security company F-Secure discovered that the results for the Ellume COVID-19 Home Test could be hacked to provide a negative result in place of a valid positive result, or vice versa.

The home test kit uses a special testing device that connects to the user's smartphone via Bluetooth. The user downloads the app, answers some screening questions, watches a video, and then performs the test. The test stick connects to the app via Bluetooth to report the test results.

EXCEPT ... a bad actor can alter the results by changing one value in the Bluetooth data after the test stick performs the test, but before it is reported to the app via the Bluetooth connection.

The Ellume home test kit, which sells at popular big-box stores (e.g. Target, Walmart, etc.) for between \$25 and \$30, is one of the tests travelers can use to enter the United States from abroad.

## Short Topix: Is The \$399 PinePhone Pro Linux Smartphone Enough To Gain Traction In Mobile Market?

With the COVID vaccine hesitancy sweeping the globe, someone with the technical ability could change a positive test result into a negative test result, which would allow them to appear as if they are not infected ... and allow them to spread the virus to many others.

### PCLinuxOS Magazine Short Topix Roundup



Just in case you haven't had enough with JavaScript on web pages you visit (think the popular NoScript browser add-on), **GET READY FOR PYTHON SCRIPTING ON THE WEB PAGES YOU VISIT.** Using the Web Assembler (WASM), according to an [article](#) on The Register, CPython scripts can run at near-native performance levels. Turning to Python helps developers overcome some limitations of JavaScript. While possessing a larger toolset than JavaScript, I can see this becoming quite a security nightmare. I could be wrong, but I don't think so.

**JIM WARREN, 85, FOUNDER OF THE WEST COAST COMPUTER FAIRE IN THE 1970'S, AND FORMER EDITOR OF DR. DOBBS JOURNAL,**

died November 24, 2021 in Silverdale, WA, from lung cancer. According to a NY Times [article](#), Warren was a leading figure in the emerging personal computing industry in the San Francisco area. After starting the first West Coast Computer Faire in 1977, it went on to become an annual event. The Apple II debuted at that first event, with Steve Jobs manning the Apple booth, with Steve Wozniak working feverishly to finish the computer in time for the show. He also went on to host the first two seasons of "Computer Chronicles" for PBS.

Starting early this year, **GOOGLE WILL BEGIN MIGRATING MULTI-LOCATION FILES IN GOOGLE DRIVE TO SHORTCUTS**, designed to simplify file and folder structures, according to an [article](#) on TechRadar. Most users will not have to do anything, and will be notified by a banner on the Google Drive page that the conversion to shortcuts is taking place.

An [article](#) from Popular Mechanics **HIGHLIGHTS SOME RECENT ADVANCES WITH LITHIUM ION SOLID STATE BATTERIES.** These batteries will have capabilities we only dream about, and will change our relationship with batteries from what we know today. For example, you will be able to charge a car that uses the new solid-state batteries in under 10 minutes. Plus, these new generations of lithium ion batteries will last 25 years or more.

**AMAZON WEB SERVICES EXPERIENCED THREE OUTAGES IN AS MANY WEEKS IN DECEMBER, 2021.** The latest AWS outage began around 4am PT/12pm GMT on December 22, 2021, with more than a thousand incident reports flagged on tracker site [DownDetector](#). The previous outage was on December 15, 2021, occurring at (or around) 09:50 am, PT. The first one occurred on December 7, 2021, around 07:00 am PT, when a network device issue caused the servers to go wonky.

**REACT OS 0.4.14**, the "open source" version of Windows (clone) was released on December 18, 2021. This update, which supersedes the last

version of 0.4.13 released in April, 2020, features significant improvements in stability, improved memory management, initial work on PAE handling, better "Plug 'n Play" support, and driver work. You can check out React OS [here](#).

**HUMANS HAVE FIGURED OUT HOW TO MAKE A WARP BUBBLE**, but don't go packing your bags just yet for the five minute trip to Mars. This warp bubble was created on a micro-scale, and isn't capable of supporting propulsion ... yet, according to a TechRepublic [article](#).



**It's easier than E=mc2**  
**It's elemental**  
**It's light years ahead**  
**It's a wise choice**  
**It's Radically Simple**  
**It's ...**



# Chrome Users Beware: Manifest V3 Is Deceitful & Threatening

by [Daly Barnett](#), EFF

Reprinted from [Electronic Frontier Foundation](#)  
Under a [Creative Commons Attribution License](#)

Manifest V3, Google Chrome's soon-to-be definitive basket of changes to the world of web browser extensions, has been framed by its authors as "a step in the direction of privacy, security, and performance." But we think these changes are a raw deal for users. [We've said that](#) since Manifest V3 was announced, and [continue to say so](#) as its implementation is now imminent. Like [FLoC](#) and [Privacy Sandbox](#) before it, Manifest V3 is another example of the inherent conflict of interest that comes from Google controlling both the dominant web browser and one of the largest internet advertising networks.

Manifest V3, or Mv3 for short, is outright harmful to privacy efforts. It will restrict the capabilities of web extensions—especially those that are designed to monitor, modify, and compute alongside the conversation your browser has with the websites you visit. Under the new specifications, extensions like these—like some privacy-protective tracker blockers—will have greatly reduced capabilities. Google's efforts to limit that access is concerning, especially considering that [Google has trackers installed on 75% of the top one million websites](#).

It's also doubtful Mv3 will do much for security. Firefox maintains the largest extension market that's not based on Chrome, and the company has said it will adopt Mv3 in the interest of cross-browser compatibility. Yet, at the [2020 AdBlocker Dev Summit](#), Firefox's Add-On Operations Manager said about the extensions security review process: "For malicious add-ons, we feel that for Firefox it has been at a manageable level....since the add-ons are mostly interested in grabbing bad data, they can still



do that with the current webRequest API that is not blocking." In plain English, this means that when a malicious extension sneaks through the security review process, it is usually interested in simply observing the conversation between your browser and whatever websites you visit. The malicious activity happens elsewhere, after the data has already been read. A more thorough review process could improve security, but Chrome hasn't said they'll do that. Instead, their solution is to restrict capabilities for all extensions.

As for Chrome's other justification for Mv3—performance—[a 2020 study by researchers at Princeton and the University of Chicago revealed that privacy extensions](#), the very ones that will be hindered by Mv3, actually improve browser performance.

The development specifications of web browser extensions may seem in the weeds, but the broader implications should matter to all internet citizens: it's another step towards Google defining how we get to live online. Considering that Google has been the [world's largest advertising company](#) for years now, these new limitations are paternalistic and downright creepy.

But don't just take our words for it. Here are some thoughts from technologists, privacy advocates, and extension developers who share our concern over Manifest V3:

*"A web browser is supposed to act on behalf of the user and respect the user's interests. Unfortunately, Chrome now has a track record as a Google agent, not a user agent. It is the only major web browser that lacks*

meaningful privacy protections by default, shoves users toward linking activity with a Google Account, and implements invasive new advertising capabilities. Google's latest changes will break Chrome privacy extensions, despite academic research demonstrating that no change is necessary. These user-hostile decisions are all directly attributable to Google's surveillance business model and enabled by its dominance of the desktop browser market." • **Jonathan Mayer, Princeton University**

"Manifest V3 positions Chrome as the all-powerful arbiter of what software lives and what dies, shattering the ideal of a diverse array of extensions serving the legitimate preferences and values of equally diverse users. In 2017, when [Google banned AdNauseam](#) from the Chrome store, it summarily cut off tens of thousands of users from data they had accumulated, and deprived them of a free and open-source extension to counter online profiling and manipulation. In hindsight, AdNauseam was the canary in the coal mine, as Mv3 is now poised to cut off users from a range of invaluable privacy tools (including ad blockers) that thousands if not millions rely on. A browser that plays favorites to advance its owners' interests effectively chokes out innovative, independent developers, while shrinking the options for individuals to shape their online experiences." • **Helen Nissenbaum and Daniel Howe (creators of AdNauseam and TrackMeNot)**

"Manifest V3 is a detrimental step back for internet privacy." • **Ghostery company blog**

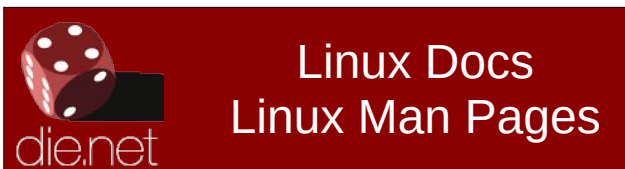
"Nearly all browser extensions as you know them today will be affected in some way: the more lucky ones will 'only' experience problems, some will get crippled, and some will literally cease to exist." • **Andrey Meshkov, AdGuard company blog**



## Screenshot Showcase



Posted by Yankee, on December 19, 2021, running Xfce.





# Log4J - What Is The Most Severe Vulnerability Of 2021?

by Alessandro Ebersol (Agent Smith)



To close out 2021, a major vulnerability has been discovered that has left the whole world on alert: the Log4J flaw.

The open source platform used by Apple, Twitter, Steam, and Tencent ventures has a serious loophole that allows malicious actors to steal sensitive data, send files to a server, and more.

According to Google, more than 35,000 Java packages, which represents more than 8% of the Maven Central repository (the main Java repository), were affected by the problem. Discovered on December 16, the vulnerability was deemed one of the "most serious" ever seen by Jen Easterly, head of the US Department of Cybersecurity and Infrastructure Security Agency (CISA).

## How do attackers take advantage of the Log4j flaw?

According to Tenable, a Cyber Exposure specialist company, the Log4J problem is considered critical because exploiting it is relatively simple. The breach allows an unauthenticated remote attacker to perform an attack on the popular Apache Log4J log library, which is used by several very popular



services such as iCloud, Amazon, and Tesla, in addition to those already mentioned at the beginning of this article.

According to Tenable, the vulnerability is exploited when an attacker sends a manipulated request that uses a Java Name and Directory Interface (JNDI injection) through a variety of services including: Lightweight Directory Access Protocol, Secure (LDAP), Remote Method Invocation (RMI), and Domain Name Service (DNS).

I have watched videos about the vulnerability myself, and it works similar to SQL injection, where it is possible to inject commands into forms.

If the vulnerable server uses Log4J to log requests, the exploit sends a malicious payload via JNDI using one of the services mentioned above, all from a server controlled by the attacker.

## What is the danger of the Log4j flaw?



Amit Yoran, cybersecurity expert and CEO of Tenable, says that this is the most critical problem of the last decade. Going even further, he argues that this is the largest vulnerability in the history of modern computing.

"This type of vulnerability is a reminder that organizations must develop mature cybersecurity programs to understand cyber risk in a dynamic world. While details are still beginning to come out, we encourage organizations to update their security controls, assume they have been compromised, and activate existing incident response plans," he comments.

According to Yoran, organizations should make it a priority to work with security and information engineering teams to drive agile responses to potential incidents and identify the internal impact of the breach.

One of the biggest risks that companies run is precisely being victims of ransomware attacks. In this type of scam, the attacker manages to encrypt the victim's information. After that, the cybercriminal charges a fee (usually in cryptocurrencies) for the data to be ransomed.

## Do users need to be worried about Log4j?

The Log4j flaw has already been fixed as of the release of patches (Upgrade to Log4j 2.3.1 (for Java 6), 2.12.3 (for Java 7), or 2.17.0 (for Java 8 and later). However, with the scope of the problem and the large number of companies affected, should the end user be concerned about the problem?

Security experts warn that applications installed on computers and other personal devices that use the

software are rare. This does not mean, however, that people can rest assured, quite to the contrary.

Besides pointing out that our personal data is "in the hands" of the various services and companies that use the open source platform, there is danger for everyone. It is necessary to create healthier digital habits.

There are no applications in the PCLinuxOS repository that use Log4J. It is more targeted to server applications, so servers are more vulnerable, and, generally, companies use old versions of Debian servers, which are not updated, and can expose these companies' servers (and their customers' data) to the flaw.



**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!*

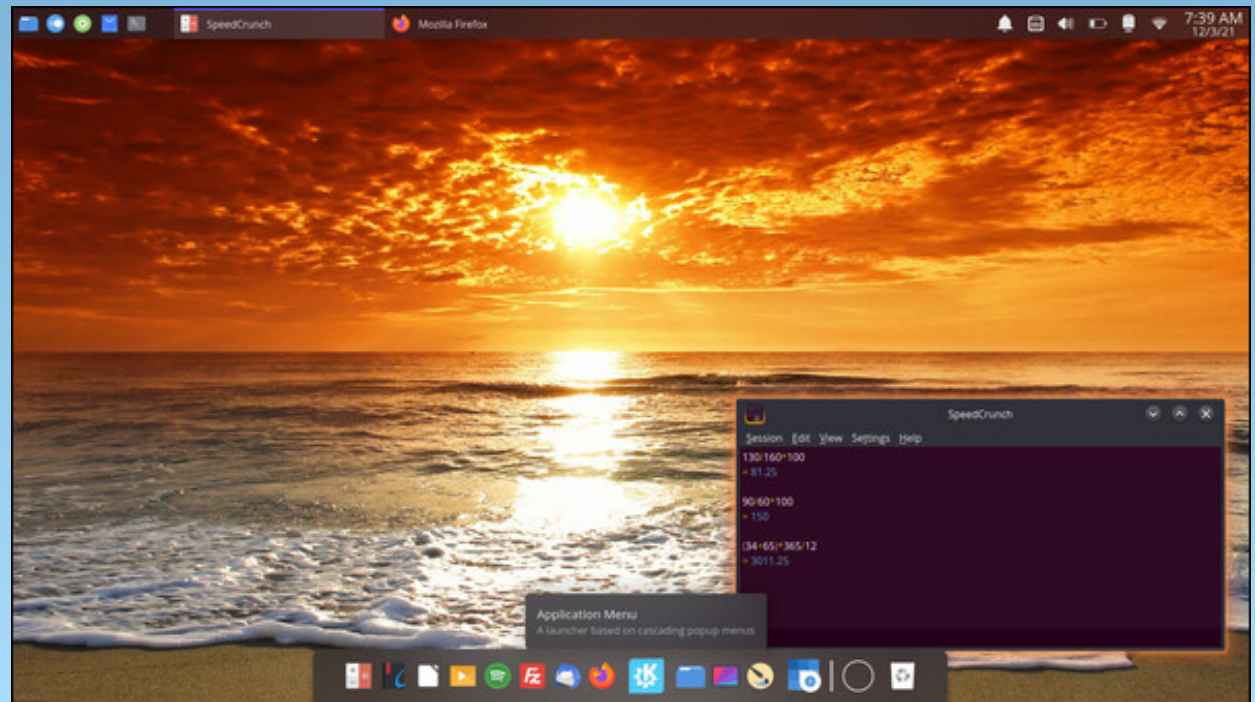


*Help PCLinuxOS Thrive & Survive*

**DONATE  
TODAY**



## Screenshot Showcase



*Posted by aguila, on December 3, 2021, running KDE.*



# PCLinuxOS Recipe Corner Bonus



## Beef and Scalloped Potatoes Casserole

Serves 6

### INGREDIENTS:

#### Beef and Potatoes

- 1 lb lean (at least 80%) ground beef
- 1 cup diced yellow onions
- 1 package (8 oz) cream cheese, cubed
- 3 1/2 cups water
- 2 boxes (4.7 oz each) scalloped potatoes

### TOPPING:

- 1 cup shredded sharp Cheddar cheese (4 oz)
- 1/2 cup chopped cooked bacon (6 slices)
- 2 tablespoons thinly sliced green onions
- Sour cream, if desired

### DIRECTIONS:

1. Spray 4 1/2- to 5-quart slow cooker with cooking spray.
2. In a 10-inch nonstick skillet, cook beef and onions over medium-high heat for 7 to 9 minutes, stirring occasionally, until brown; drain. Return beef mixture

to skillet, and place over low heat; stir in cream cheese. Cook for 2 to 3 minutes, stirring frequently, until cream cheese melts.

3. In a slow cooker, mix water and sauce mixes (from scalloped potato boxes), then stir in potatoes (from scalloped potato boxes). Spread beef mixture over potatoes.

4. Cover; cook on Low heat setting 2 to 2 1/2 hours or until potatoes are tender and liquid is absorbed.

5. Stir mixture. Top with Cheddar cheese; cover, and cook on Low heat setting 3 to 5 minutes longer or until cheese is melted. Top with bacon and green onions. Serve with sour cream.

### Expert Tips

To test potato tenderness without releasing too much heat from the slow cooker, slightly lift the lid, and slide a bamboo skewer into the center of the mixture. Potatoes should be very tender.

To ensure even cooking of potatoes, make sure to fully cover potatoes with beef mixture.

### NUTRITION:

Calories: 274  
Fiber: 1.0g  
Protein: 23.5g

Carbs: 20.4g  
Sodium: 588.4mg



**The PCLinuxOS  
Magazine**

**Created with  
Scribus**

# U.K. Proposal To 'Bcc' Law Enforcement On Messaging Apps Threatens Global Privacy

by **Paulo Garcia**, Assistant Professor, Carleton University

Reprinted from [The Conversation](#)

Under a Creative Commons [Attribution/No derivatives](#) 4.0 license



The term “ghost protocol” might remind you of a famous blockbuster starring Tom Cruise, but here it applies to a new proposal by the Government Communications Headquarters (GCHQ) in the United Kingdom.

The GCHQ is the British equivalent of the [United States National Security Agency](#), and the proposal's function is to give law enforcement power to [listen in on encrypted communications](#) (like those on WhatsApp, for example).

It's not the first time the British government has taken aim at encrypted communication: in 2017, then Home Secretary Amber Rudd called for [end-to-end encryption to be banned](#), claiming “real people” don't need it. Rudd's comment reflected tremendous ignorance about how modern communication works.

The proposal, referred to informally as ghost protocol, is a more strategic attack on privacy, packaged in security rhetoric that hides technical,

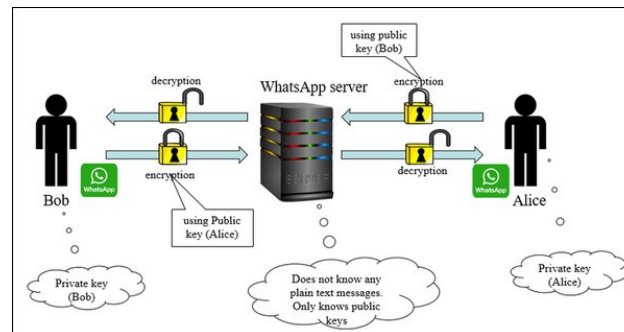
personal and societal implications. In an [open letter to GCHQ](#), 47 signatories — including Apple, Google and WhatsApp — have urged the agency to abandon its plans.

## How end-to-end encryption works

The government proposal says “[you don't even have to touch the encryption](#)” to implement ghost protocol. [End-to-end encryption](#) works by generating a pair of public and private keys for each user. Text encrypted using the public key can only be decrypted using the private key, and vice versa.

Hence, if Bob and Alice want to have a chat, both share their public keys and keep their private keys secret. Bob encrypts messages using Alice's public key (so only Alice can decipher them), and Alice encrypts messages using Bob's public key.

In a group chat between Alice, Bob, and Jill, every message Alice sends is encrypted using Bob's public key (to Bob) and Jill's public key (to Jill). Alice is notified by the app that each message has two recipients. This means that the messaging service's servers only see public keys and encrypted text: they cannot decipher text, even at the request of law enforcement.



How end-to-end encryption works.

## Ghost in the machine

Ghost protocol gets around this problem by proposing that law enforcement can be added as an invisible participant to a conversation. Alice, in conversation with Bob, would then encrypt every message twice, using both Bob's public key and the public key for law enforcement. Alice would be unaware of law enforcement's ability to access her conversation.

Framing this as an action that could only be taken if legally approved and only in situations where there is sufficient evidence to justify it sounds reasonable, but ghost protocol completely disregards the [many technical implications](#) of modifying software to support a ghost user.

It would require messaging apps to change [how keys are negotiated among participants](#), adding complexity and therefore increasing the potential for security vulnerabilities.

By requiring apps to hide participants, it would undermine authentication mechanisms, introducing new potential vulnerabilities and eroding user trust in the service.

It would also effectively create [a backdoor](#) that could be exploited by messaging apps themselves — for example, a company employee who wants to stalk a co-worker. This would create a single point of failure: should a malicious attacker hack into the messaging app system, they would then be able to inject themselves as a silent listener into any conversation.





## Social implications

The personal and societal implications are even more serious. Messaging apps would need to update their software to support ghost protocol. Would this update affect all users, regardless of geographical location? Would a Canadian user be affected because a messaging app update implements U.K. law? This opens the door to any government, including dictatorships, to spy on their citizens effortlessly and covertly.

Remember the [Edward Snowden leaks](#)?

If two versions of the software existed — one for users in the U.K., one for everywhere else — how would these inter-operate? Would a Canadian visiting the U.K. be able to use the messaging app? Probably not, without an update that incorporates ghost protocol. That update that would remain on their phone after they returned home.

Law enforcement definitely needs access to information to provide security and prosecute crimes, and technology has certainly made this more challenging. But law enforcement's intelligence-gathering capabilities cannot be supported by undermining individuals' right to privacy, which is what ghost protocol proposes. It makes the many more vulnerable, so the U.K. can spy on a few.





## PCLOS-Talk

Instant Messaging Server

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



## Screenshot Showcase



Posted by brisvegas, on December 1, 2021, running Mate.

# PCLinuxOS Puzzled Partitions

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

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

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

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

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



## SCRAPPLER RULES:

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

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

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

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

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

0 points: 2 blank tiles

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

2 points: D, G

3 points: B, C, M, P

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

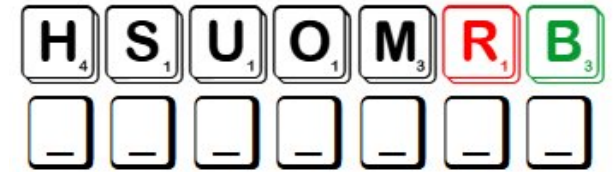
5 points: K

8 points: J, X

10 points: Q, Z

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

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



Triple Word



Double Word



Possible score 253, average score 177.

Download Puzzle Solutions Here



# ***PCLinuxOS Word Find: January, 2022***

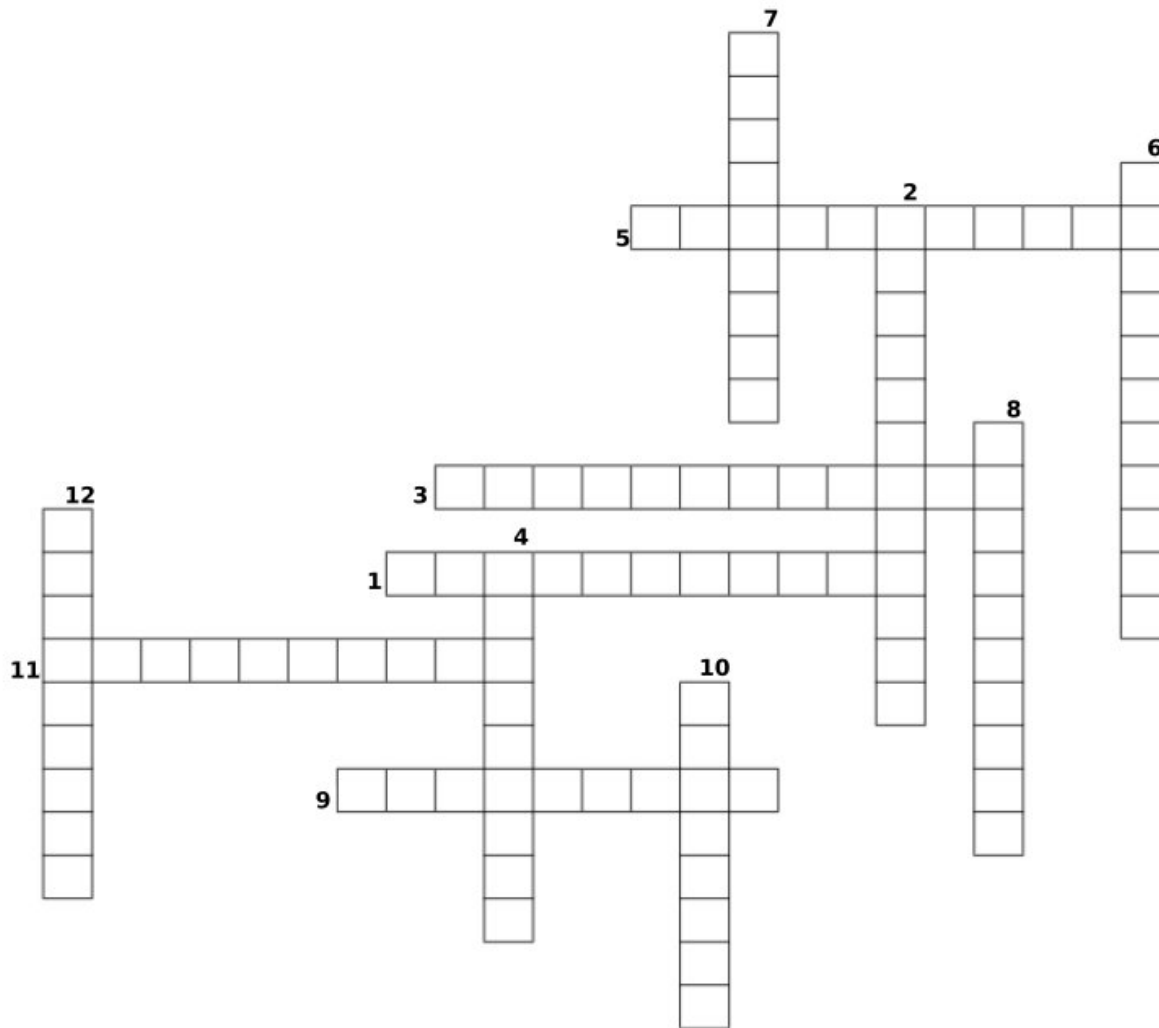
## ***New Year's Eve***

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

AULD LANG SYNE	BALLOONS
BUBBLY	CALENDAR
CELEBRATION	CHAMPAGNE
CHEERS	CLOCK
CONFETTI	COUNTDOWN
DANCING	DECEMBER
EXTRAVAGANZA	FATHER TIME
FESTIVITIES	FIREWORKS
GAMES	GATHERING
HAPPY	HOLIDAY
HOURLASS	INVITATION
JANUARY	KISSING
MEMORIES	MERRYMAKING
MIDNIGHT	MUSIC
NEW YEARS EVE	NOISE MAKER
PARADE	RESOLUTIONS
SPARKLERS	STREAMERS
TWELVE OCLOCK	

[Download Puzzle Solutions Here](#)

# New Year's Eve Crossword



1. A firm decision to do something or a course of action decided on.
2. A popular song, traditionally sung to bid farewell to the old year.
3. An elaborate, spectacular entertainment, celebration or display.
4. Long narrow strips of material used for ornament or decoration.
5. The last day of December.
6. Joyous feasts, holidays, or celebrations.
7. Bottle rockets, fountains, sparklers and the like....
8. A character symbolizing the end of the year.
9. A carbonated alcoholic beverage used for celebrations.
10. Very small bits of paper used for celebration.
11. An instrument, such as a clapper, horn or bell, designed to add to a celebration.
12. The counting backward aloud from an arbitrary starting number to indicate the time remaining before an event or operation.

[Download Puzzle Solutions Here](#)



# Mixed-Up-Meme Scrambler



"We're spending our honeymoon at a  
 \_\_\_\_\_  
 instead of one of those expensive hotels."

Sealed  
**LOCEKD**

   \_\_\_\_\_

Beached  
**ROAHSE**

  \_\_\_\_\_

Fangs  
**TEHET**

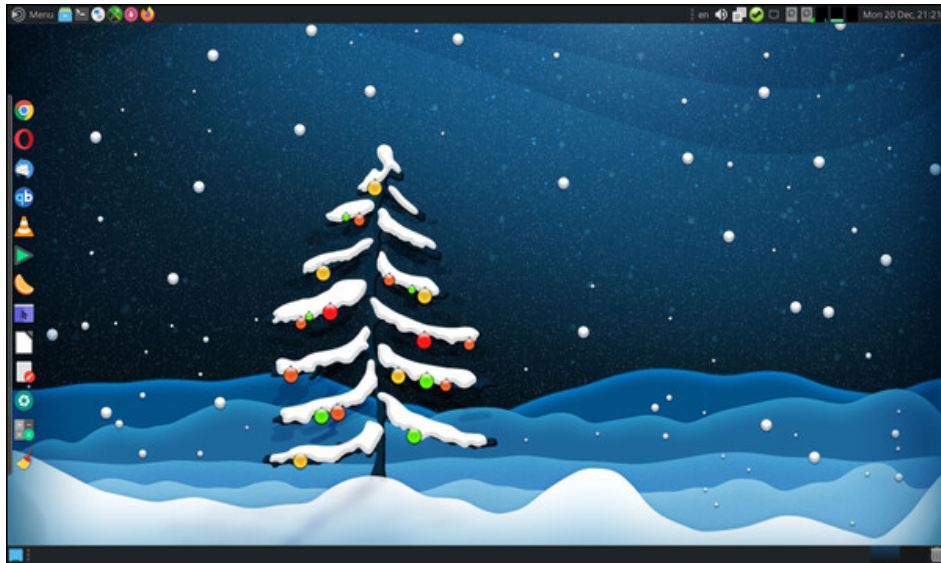
 \_\_\_\_\_ 

Digger  
**HEOVLS**

 \_\_\_\_\_  \_\_\_\_\_ 

Use the clues to unmix the letters to  
 make a new word. Remix the letters in  
 the red boxes to solve the puzzle.

# More Screenshot Showcase



Posted by jogurtmen, on December 19, 2021, running Mate.



Posted by Meemaw, on December 17, 2021, running Xfce.



Posted by mutse, on December 13, 2021, running Mate.



Posted by OnlyHuman, on December 17, 2021, running e24.