

# The PCLinuxOS magazine

Volume 188

September, 2022



# In This Issue...

- 3 *From The Chief Editor's Desk...*
- 4 *Screenshot Showcase*
- 5 *OTA Broadcast TV With Kaffeine*
- 12 *Screenshot Showcase*
- 13 *PCLinuxOS Recipe Corner:  
Chicken & Rice Casserole Foil Packs*
- 14 *Online Platforms Should Stop Partnering With  
Government Agencies To Remove Content*
- 16 *Art Project In GIMP 2022*
- 19 *Screenshot Showcase*
- 20 *Repo Review: Rapid Photo Downloader*
- 21 *Bad Data "For Good": How Data Brokers Try To Hide  
Behind Academic Research*
- 23 *Short Topix: New Free, Open Source AI Tool Can Fix Most  
Old Photos In Seconds*
- 29 *Screenshot Showcase*
- 30 *GIMP Tutorial: Make A Shadow Using Your Subject*
- 31 *Screenshot Showcase*
- 32 *Nonprofit Websites Are Full Of Trackers. That Should Change.*
- 34 *Screenshot Showcase*
- 35 *PCLinuxOS Bonus Recipe Corner: American Goulash*
- 36 *PCLinuxOS Puzzled Partitions*
- 40 *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

daishi

Cg\_Boy

YouCanToo

Pete Kelly

Smileeb

Alessandro Ebersol

**Contributors:**

tuxlink

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

When you consider the vastness of the universe, it's difficult to comprehend how little, miniscule "events" come together. That's exactly what happened to me recently.

We (finally) got a chance to take our new camping trailer out on its inaugural camping trip. We chose a campground close to home for the initial "shake down" trip. Our location had a lake, and a short bike path that went all the way around the lake. We love riding bikes, so this campground was especially selected because of its bike path. It gives the kids something to do that they love.

On our bike rides, it's usually me out front. I like to go fast, while my wife likes to go at a much more leisurely pace. So, I usually ride ahead, and then stop and wait for her to catch up. My son is determined to keep up with dad, so he's usually the second one in our little bike parade. My daughter takes the third position, while my wife brings up the rear.

The bike path around the small lake is 3.75 miles (6.04 Km) long. Including the distance from our campsite, our bike ride would total 5.62 miles (9.04 Km) long (measured with my smart watch's GPS, which I started when we began our ride). We're accustomed to much longer bike rides, so this one was definitely within the realms of our abilities. Before the kids came along, my wife and I would go on bike rides of between 30 and 50 miles (50 to 80 Km) pretty regularly. Since the kids have come along (and since they've learned to ride their bikes), the longest bike ride we've been on is around 12 miles, or 19.3 Km.

So, we're riding in our usual fashion, with me out front, followed by my son, then my daughter and wife bringing up the rear. We're about half of the



distance around the lake. That is, it's just as far to turn around and go back as it is to continue going forward.

Since I like to go fast, I frequently breathe with a slightly open mouth to help increase air movement in and out of my lungs. This day, apparently, was not the day to do that.

So, I'm going down a small hill, and really gaining some speed. I'm pedaling through the downhill slope, hoping to gain an extra amount of speed to get back up the hill on the other side. All of a sudden, about half way down the hill, a bug flew into

my partially opened mouth. Yeah, I can already hear the jokes about that one!

So I'm coughing, gagging and sputtering about, trying to get the flying intruder out of my mouth. Now it's starting to actually hurt. My son comes up and says, "Hey, Dad! What's wrong?" I told him a bug flew into my mouth, and I was trying to get it out. He pointed down on the ground, and said "There's a yellow jacket!" Sure enough, there was a yellow jacket. He (the yellow jacket) looked quite confused and dazed, like "what the heck just happened to me?"

A yellow jacket is the “bug” that flew into my mouth! It scared the shiitake mushrooms right out of me! I’ve been stung by these evil flying devil insects before, and have had a reaction to them in the past. This “bug” had managed to START to sting me at the back of my mouth before I got him coughed and sputtered out of my mouth. The only thing I had with me (medication-wise) were some ibuprofen tablets. I took a 600mg dose and continued on my way. Being literally midway around the lake, what else could I do? And hurt? It was THROBBING at this point! By the way, I was the LAST thing that he ever stung. I ground him into the asphalt paving of the bike trail with my foot.

Let me tell you something. Getting stung on the INSIDE of your mouth by a yellow jacket is generally considered a medical emergency. The risk of your airway swelling shut is very, very real. This is why I was very, very scared. “Airways” have been my “business” for the past 35 years as a respiratory therapist. I am/was very cognizant of the risk(s) from being stung in the mouth by those evil flying devil insects!

We made it back to the camping trailer without further incident. In fact, the picture above was shot after the yellow jacket incident, when we were about three-quarters of the way around the lake. I did drive into town to get some more ibuprofen, acetaminophen, and some Benadryl after we got back. I took the Benadryl before I went to bed that evening, and awoke the next morning feeling much better. The antihistamine was exactly what I needed to counter the sting. Oh, I could still feel it. In fact, I could still feel the after-effects of the sting for another few days, in fact. But the swelling risk had passed, and I could (literally) breathe easier.

In all the universe, what are the chances that an evil flying devil insect, a yellow jacket that measures less than 1 inch long (2.54cm), would find its way into my slightly agape mouth (less than 6cm)? There has to be infinitesimally small odds for something like that to happen! I’m just glad to have gotten him coughed

out before he had a chance to get a really good sting on me. I think things would have been a LOT more serious if he had actually gotten a good sting on me. Lucky? Maybe, but I’m not known for having much luck of the “good” variety.

\*\*\*\*\*

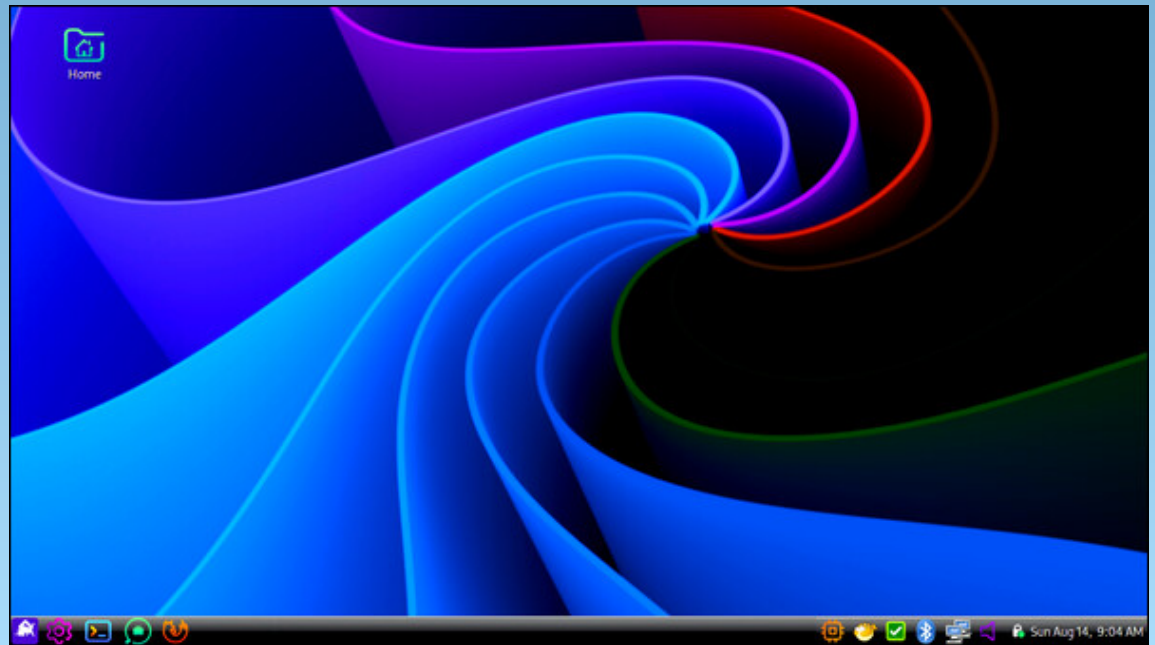
This month’s cover, designed by Meemaw, celebrates International Bacon Day, on September 3, 2022. The “unofficial” [holiday](#) is celebrated annually on the first Saturday of September.

\*\*\*\*\*

Until next month, I bid you peace, happiness, serenity, prosperity, good health ... and NO stinging insects!



# Screenshot Showcase



Posted by Upgreyed, on August 14, 2022, running Mate.



# OTA Broadcast TV With Kaffeine

by Paul Arnote (parnote)



As I promised last month, I'm winding up my series of articles on how to watch OTA (over the air) TV broadcasts on your PCLinuxOS computer. You will, of course, have to have the hardware (or access to the hardware ... namely, a TV tuner card/dongle that's [supported](#) under Linux) to be able to receive these broadcasts, hooked to an antenna/aerial or cable TV input.

In the July issue of The PCLinuxOS Magazine, I [covered](#) how to use VLC to receive and watch OTA TV broadcasts. I included a bash script to make it easier to scan for the channel information and save it to a file that can be loaded into VLC at will. In the August issue of The PCLinuxOS Magazine, I [covered](#) how to use MPlayer to receive and watch OTA TV broadcasts. I included two bash scripts with that article. One was to simplify scanning for channels, and the other was to make it easier to watch those TV stations with MPlayer.

If you are one of those Linux users who prefer to avoid the Linux command line and/or bash scripts, you will be relieved to know that by using Kaffeine to view OTA TV broadcasts, you won't have to mess with any of that. By far, Kaffeine is the EASIEST to use to watch OTA TV broadcasts. All of the abilities are built into Kaffeine for scanning for the channels available in your area, and then watching them.

So, to get started, let's take a look at Kaffeine's description from the LinuxTV.org [Wiki](#):

*Kaffeine is a media player. What makes it different from the others is its excellent support of digital TV (DVB). Kaffeine has a user-friendly interface, so that even first time users can start immediately playing their movies: from DVD (including DVD menus, titles, chapters, etc.), VCD, or a file.*

*Kaffeine version 2.0, launched in June 2016, has its GUI written on the top of KDE Frameworks 5 and Qt5. For video/audio playback, it uses libVLC as its backend, and it interfaces with Linux TV devices via libdvbv5.*

*It has a simple but intuitive interface and is easy to set up. Amongst its list of supported formats are CDDA, VCD, DVD, ... and, since versions >0.5, it also provides full DVB support.*

**The latest version is 2.0.3.**

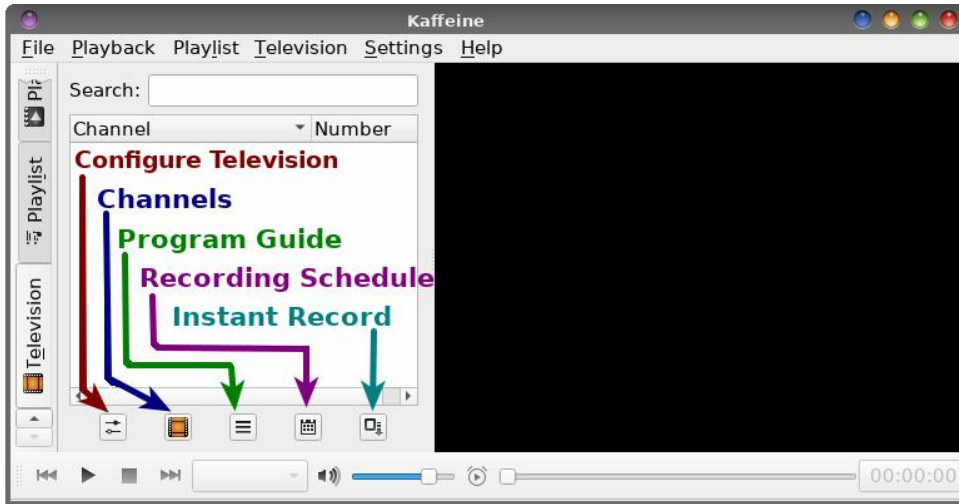
Yes, Kaffeine is a complete multimedia program. With it, you can playback your multimedia files, audio CDs, video CDs (I haven't seen nor created one of those in about 20 years ... I didn't even realize that they were still a "thing"), DVDs, and digital TV. But, for this article, we're going to focus on its ability to play digital OTA TV broadcasts on your desktop.

## Getting Started

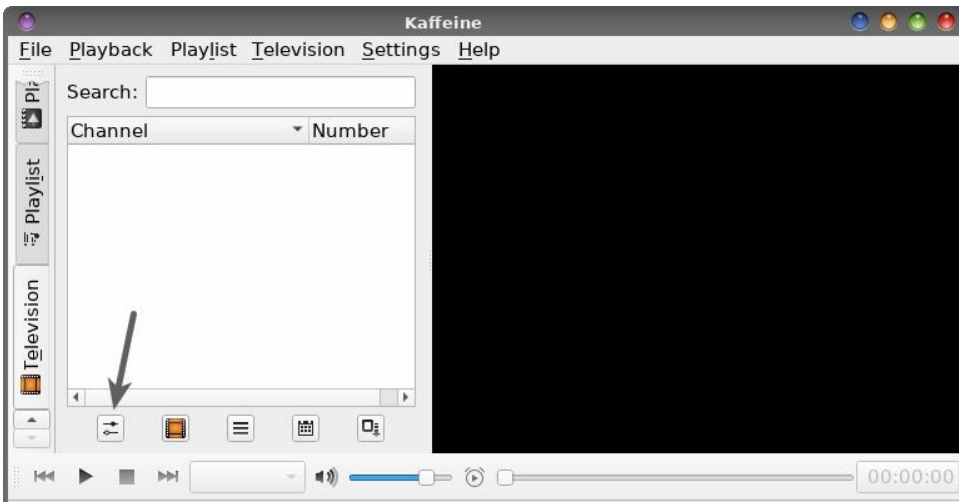


When you first launch Kaffeine, you should see something similar to the image above (bottom of right column, previous page). To get started watching OTA TV broadcasts, you will click on the “Digital TV” button.

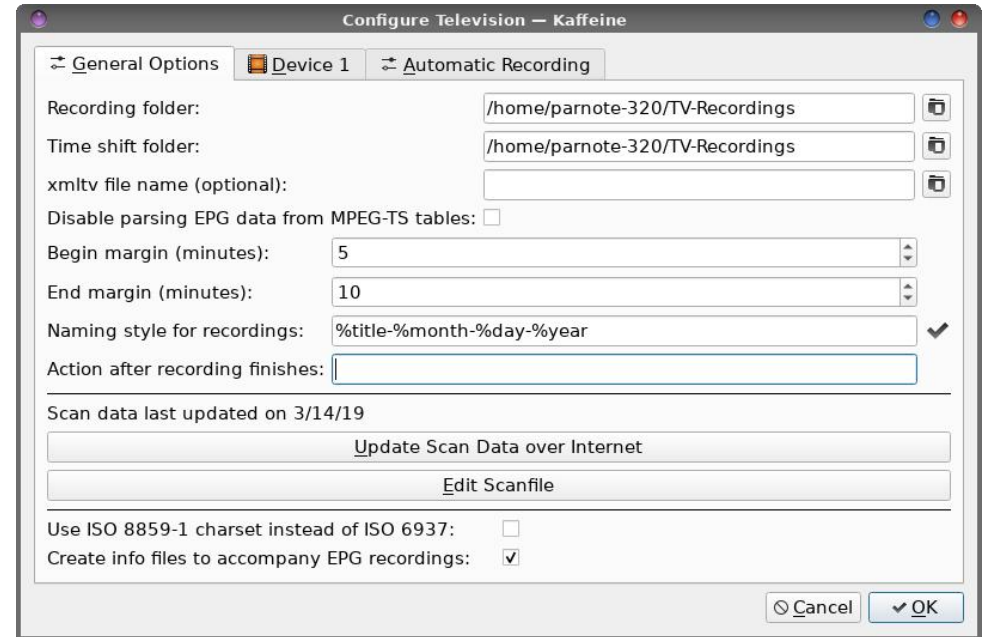
For a quick reference, here’s a “key” of sorts for the important buttons in the Digital TV window of Kaffeine.



Before we can really get down to business, we will need to make a few configuration settings for the digital TV portion of Kaffeine.



Click on the settings button at the lower left part of the Kaffeine window, indicated by the gray arrow (image bottom of previous column). Alternatively, you can select the Television > Configure Television... menu item.

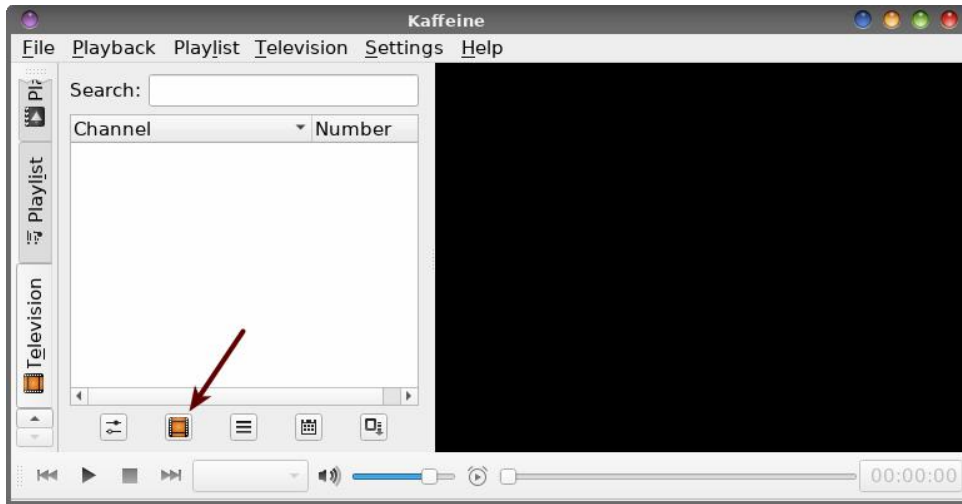


You will need to set the “Recording folder” and “Time shift folder” for where your recordings and timeshift recordings will be stored. I created a folder in my /home directory, called TV-Recordings, and then used that.

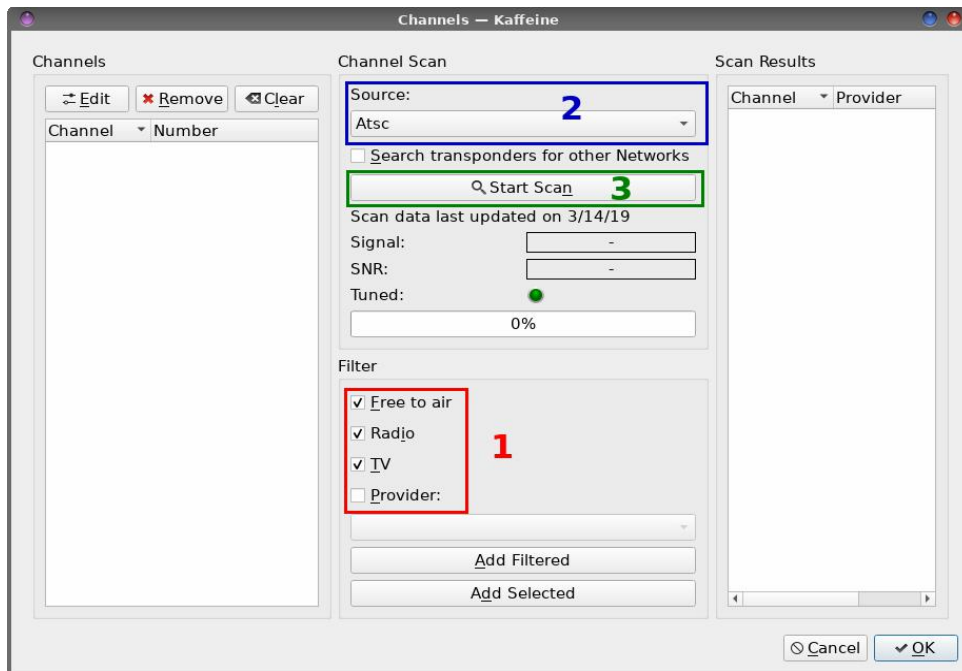
You might also want to adjust the “Begin margin” and “End margin” settings. By default, they are set to begin recording five minutes before the scheduled program time, and to end ten minutes after the program’s scheduled end time. That’s too much for my tastes, so I change these to two minutes each. That is, I set the recording to start two minutes before the scheduled start time, and to end two minutes after the scheduled end time. For most cases, that should be sufficient.



## OTA Broadcast TV With Kaffeine

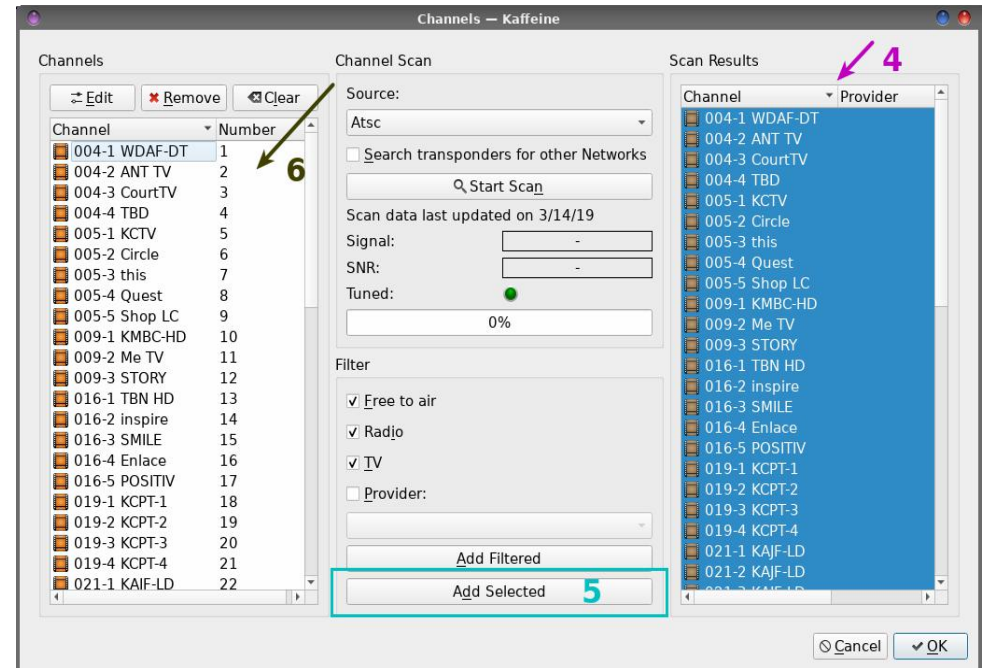


When you click on the “Digital TV” button, you should see something like the image above appear. Even though it doesn’t look promising, don’t fear. This couldn’t possibly be any easier. We haven’t scanned for OTA TV broadcasts in our area yet. To do so, click the button at the lower left of the window indicated by the arrow. Alternatively, you can also select the Television > Channels menu item.



Clicking on the Channels button from the previous window (or selecting the Television > Channels menu item) will lead you to the window shown above. For your convenience and to make it easier to follow along, I’ve numbered each step in the image.

First, you need to select what you want to search for. Here, I’ve selected “Free to air,” “Radio,” and “TV” as the filter criteria. Second, you need to be sure to select the broadcast standard for your area. Since I’m in the U.S., my broadcast standard is ATSC. In other parts of the world, it will most likely be DVB-T or DVB-T2. Third, click on the “Start Scan” button. This will take a few minutes, so sit back and relax while Kaffeine scans for OTA TV broadcasts in your area.

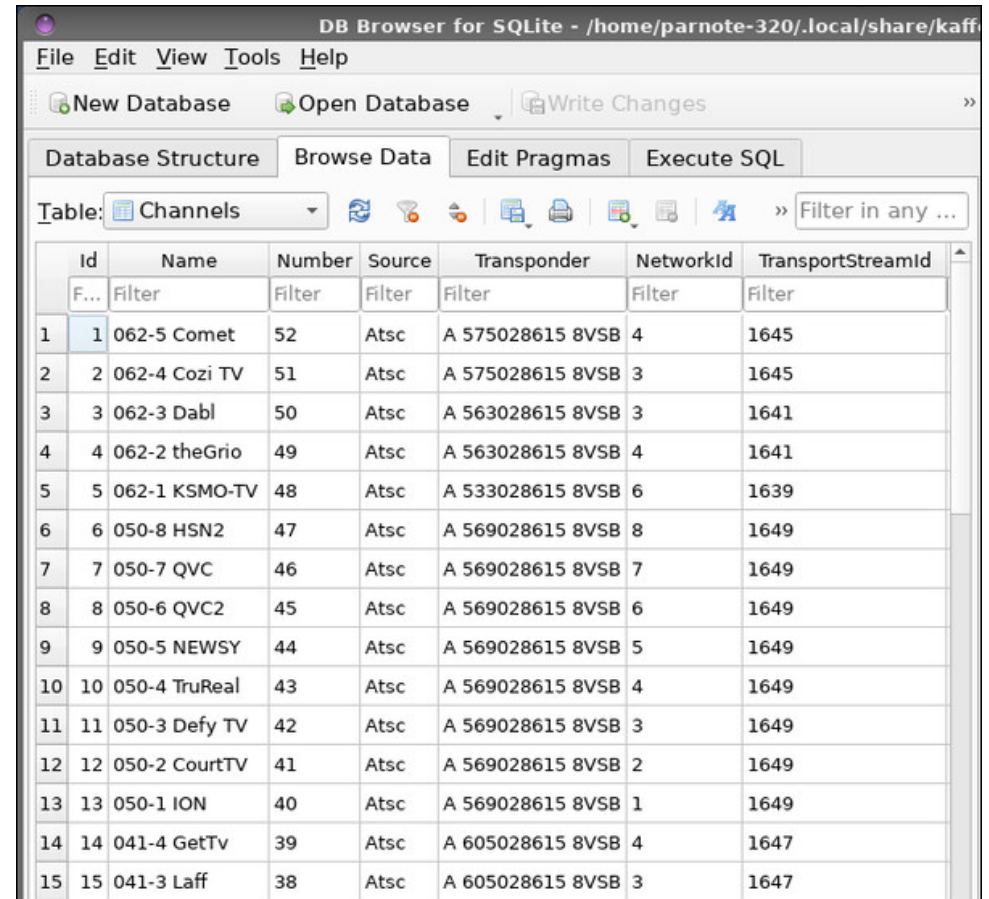


Fourth, once the scan is complete, click on the first TV channel listed in the listbox on the right side of the window, and then press Ctrl + A on the keyboard to select all of the channels. Fifth, click the “Add Selected” button at the bottom center of the window. The selected OTA TV channels will then be added to your Channels listbox on the left side of your window (item 6). Finally, select the OK button at the lower right corner.



Now, just double click your mouse cursor over the OTA TV channel you want to watch, and the OTA TV broadcast should appear in the playback area on the right half of the Kaffeine window.

To change channels, simply double click on the new channel you want to watch. If you just want to “surf the channels,” use the “Previous” and “Next” buttons in the lower left corner of the Kaffeine window. For a while, at least, you might want to “surf the channels.” I have to admit that I never knew many of these channels even existed. At home, we have digital cable TV, and it seems that my cable system doesn’t include many of these channels. So, by “surfing the channels,” you get the opportunity to see if the channel’s programming is something you might be interested in. But please ... don’t get hooked on the shopping channels that are on the OTA TV broadcasts. Your bank account will thank you. In my area (the Kansas City area), there are no fewer than seven different OTA TV shopping channels being broadcast at any given moment. Geez! I thought their popularity candles blew out long ago.

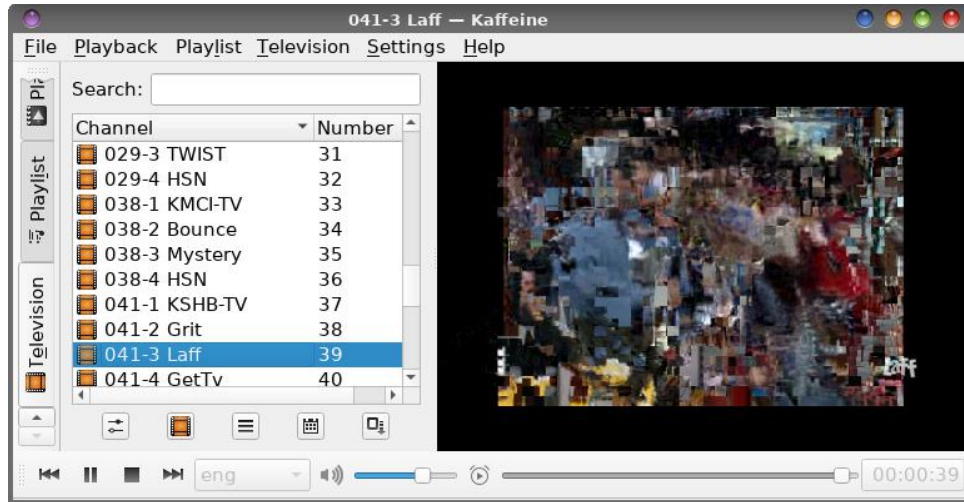


So where does Kaffeine save the results of the channel scan? This one had me extremely puzzled for a long time. I actually spent HOURS picking through the Kaffeine source code, to no avail, to figure out where the channel scan results were stored. Finally, with the help of Only16 (via a private chat on PCLOS-Talk), the location was found. Those results are stored in the `~/local/share/kaffeine` directory, in a file called `sqlite.db`. This file is not readable in a text editor, at least in any kind of readable manner. To view this file, you have to install the `sqlitebrowser` package from Synaptic. Then, load in the `sqlite.db` file into `sqlitebrowser`, and go to the “Browse Data” tab (image above). Tada! There they are! I’m not sure what the advantages are of storing the channel scan data in a binary `sqlite` database file versus a text file, but it does seem a bit like overkill to me. Curiosity can lead to a lot of wasted time. And, even though it does seem rather excessive to me versus a regular text file, I’m just glad to have found it and that it works. Plus, it reminded me how much I hate reading C++ source files





(which is what Kaffeine is written in), because I could never get a handle on C++. With “regular” C, I’m good. But not with C++.



Also, don't be surprised if you're not able to view every channel that the channel scan detects in your area. As shown in the image above, weak stations may appear as pixelated blobs on your desktop. It's part of the gamble. Receiving some channels may require a reorientation of your antenna/aerial in order to receive an adequately strong signal. Some things you can try include moving your indoor antenna/aerial to a window, or raising the elevation of your antenna/aerial. For some, you may never receive an adequately strong enough signal to avoid the pixelated mess on your screen. In my area, we have seven low power, low definition channels that my channel scans detect (there are more in my area that are never detected), and being able to tune in to any of them is truly hit or miss.

There are other factors to consider, as well. Weather systems and sun spot activity are two variables. Terrestrial terrain is important, too. Having a few hills or mountains between you and the broadcast tower can severely limit decent reception, since OTA TV broadcasts are generally “line of sight.” That means signals go in a straight line, and don't bend to adapt to the terrain. Thus, having hills or mountains between you and the signal can seriously degrade reception signal strength. Distance from the tower is a factor, also. In the image above, that broadcast signal originates from a broadcast tower that's about nine miles (about 14.5 Km) from me, with several hills in between me and the tower.

In the U.S., you can check out the OTA TV broadcast towers near you by visiting [OTADTV.com](http://OTADTV.com). There, you can put in your address, and a map with all of the OTA TV broadcast towers will be displayed for your area. This is also how I know that

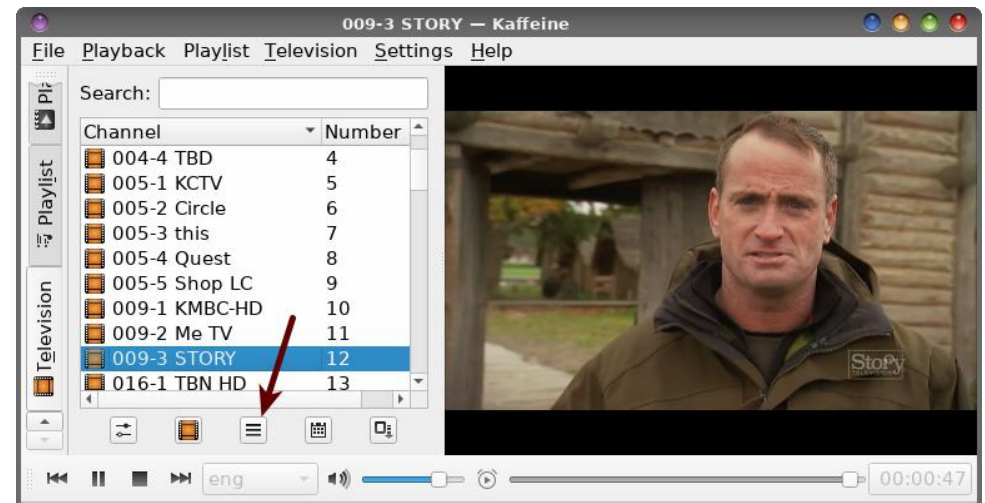
there are more low power, low definition OTA TV broadcast towers near me that are never detected in a channel scan. The map will also display how far away the broadcast towers are from your location ... as a crow flies (straight line radius).[a]

My current setup is less than ideal. To be perfectly honest, my USB TV tuner dongle is attached to my laptop in my living room, on the coffee table. The antenna/aerial is propped up behind my laptop's lid. Without a doubt, I would get a much better signal if I were to at least reposition the antenna/aerial in the window. But for now, this is good enough for my use.

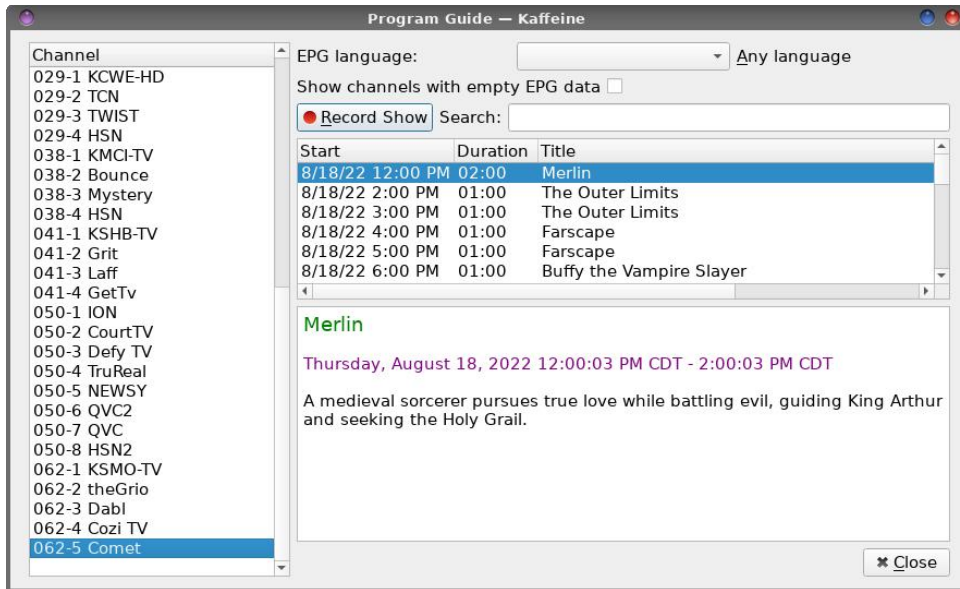
Also at the bottom of the playback window is your volume control. Click on the little sound icon to mute or unmute the sound. Slide the control to the right to increase the volume, or slide the control to the left to decrease the volume. Alternatively, you can hover your mouse cursor over the playback window, and then scroll with the mouse wheel to raise or lower the volume.

### Diving Deeper: There's More

Kaffeine also has an EPG, which is short for “Electronic Program Guide.” That information is usually sent out on the OTA TV broadcast signal, from what I can tell.



To access the EPG, click on the third button from the left in the group of buttons at the lower left half of your Kaffeine window (indicated by the arrow in the image above). Alternatively, you can select the Television > Program Guide menu item, or just hit the “G” key on your keyboard, which is set up to be the hotkey for Kaffeine to access the EPG.



The EPG will open to the channel you are currently watching. It will (most likely) have the entire day's worth of programming for that given day. Don't worry when opening the EPG for the first time if hardly any channels appear in the listbox on the left side of the window. These will fill in as you watch more channels.

If you want to peruse what's on, just single click the channel in the left-side listbox, and that channel's programming data will be displayed. You cannot change channels from here, but you can see what's on.

Some stations do not have EPG data at all. In my area at least, I've found that the low-power low-definition stations do not have EPG data available.

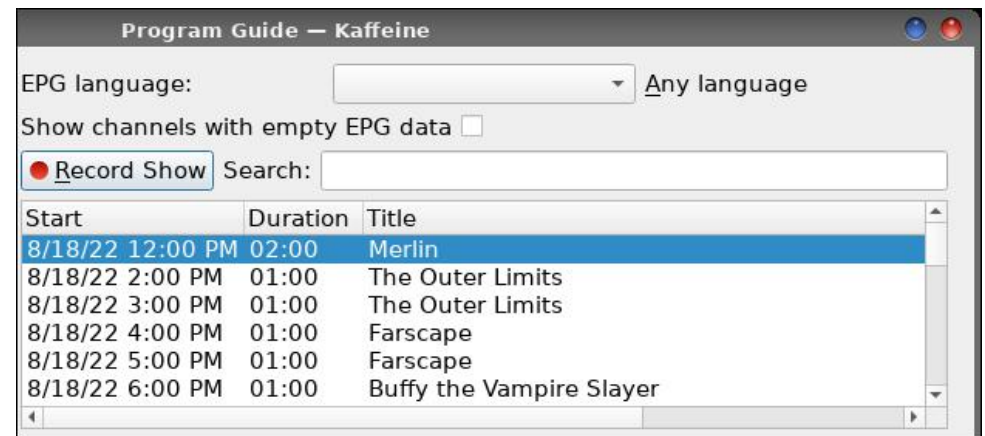
As you can see from the image above, the start times of the shows are displayed, along with the length of each show. When available, a brief description is available for the selected show in the programming guide in the bottom right pane of the window. That is usually the case, but in some cases, no descriptions are available. I've found this to sometimes be the case on channels like Antenna TV, where they show programming from the classic days of television ... otherwise known as old shows, like Dennis the Menace, Bewitched, That Girl, and Welcome Back Kotter.



## And Even More ... Recording & Time Shifting

You might have noticed the record button in the last section discussing the EPG. Or you may have noticed that we talked about setting the directory and start/end times for recordings. Yes, Kaffeine makes recording OTA TV broadcasts a trivial matter.

Regardless of how trivial it is, I do have to warn you. These recordings will consume a LOT of hard drive space. So, be sure you have plenty of available hard drive space before making your recording(s). Recording a 30 minute show (which is actually 34 minutes, with my recording "margins" set to two minutes before the show starts to two minutes after the show's scheduled stop time) consumes just over 500MiB of hard drive space. So, that means – on average – one hour of video comes in at about 1GiB of hard drive space.



The easiest way to record a show is to go to the EPG window, select the show you want to record, and then hit the "Record Show" button. When you do, a red dot will be placed before the show title to indicate that it is scheduled to be recorded. The recording will be placed in the directory that you specified when you set up Kaffeine's Television settings.

The other way to record an OTA TV broadcast is to hit the "Instant Record" button in the row of buttons at the bottom left of the Kaffeine window. It's the last/fifth button on the row, just below the channel listing. Clicking it once will start the recording, and change the button's appearance to a large red dot. Clicking it again during the recording will cause the recording to stop. It hardly gets any simpler than that.

Despite various reports that Kaffeine will allow you to record one program while watching another, that isn't necessarily true. And, for all I know, it may just

depend on what hardware you have. I know that with my KWorld ATSC USB Tuner dongle, you cannot record one thing while watching another. But, for recording a show while I'm away, it works perfectly ... as long as I leave Kaffeine up and running. That isn't a problem for me, since I typically leave my computers on 24/7.

Kaffeine records the program(s) as m2t files. If you're not familiar with those types of files, those are MPEG2 transport stream files. Those files are not necessarily the most economical file format when it comes to file size. So, using a [bash script](#) I wrote several years ago, I converted the m2t file to a MP4 file that uses H.264 compression. In doing so, I reduced the size of the m2t file from 502.0MiB to a MP4 file of 276.0MiB. That's a 45% reduction in file size, which is significant. At least to my eyes and ears, I can't perceive any degradation in image or sound quality with the MP4 file compared to the m2t file.

Of course, there are a LOT of variables involved with how big the MP4 file is, and one of the biggest is the video bitrate setting. Lower video bitrates mean smaller files, and vice versa. The video bitrate for the MP4 file in my example here was set to 1000kbps. The quality is decent. By raising the video bitrate on the conversion to 2000kbps, the MP4 file is a similar size as the m2t file. I'll have to leave it up to you to decide what quality level you want for the video, versus how much you'd like to reduce the file size. I've covered video bitrates multiple times over the years, so I'm not going to go over it again here. I've nothing more to add to what I've written in the past. The previous articles are easy enough to find by using the DuckDuckGo [search](#) feature on the magazine's website.

**Summary**

So, as I mentioned earlier, Kaffeine is the absolute easiest program to use to watch and/or record OTA TV broadcasts. In my experience with it, Kaffeine has worked its way to being my choice program to use for either watching or recording OTA TV broadcasts, supplanting VLC as my previous go-to program. Don't get me wrong. I still love VLC, but Kaffeine makes the whole process so much easier.

## The PCLinuxOS Magazine Special Editions!

**Get Your Free Copies Today!**

**PCLinuxOS-Cloud** secure private simple-to-use  
 Sign up TODAY! [pclosusers.com/services-signup.php](http://pclosusers.com/services-signup.php)

Help PCLinuxOS Thrive & Survive

**DONATE TODAY**





Support PCLinuxOS! Get Your Official

**PCLinuxOS**  
Merchandise Today!

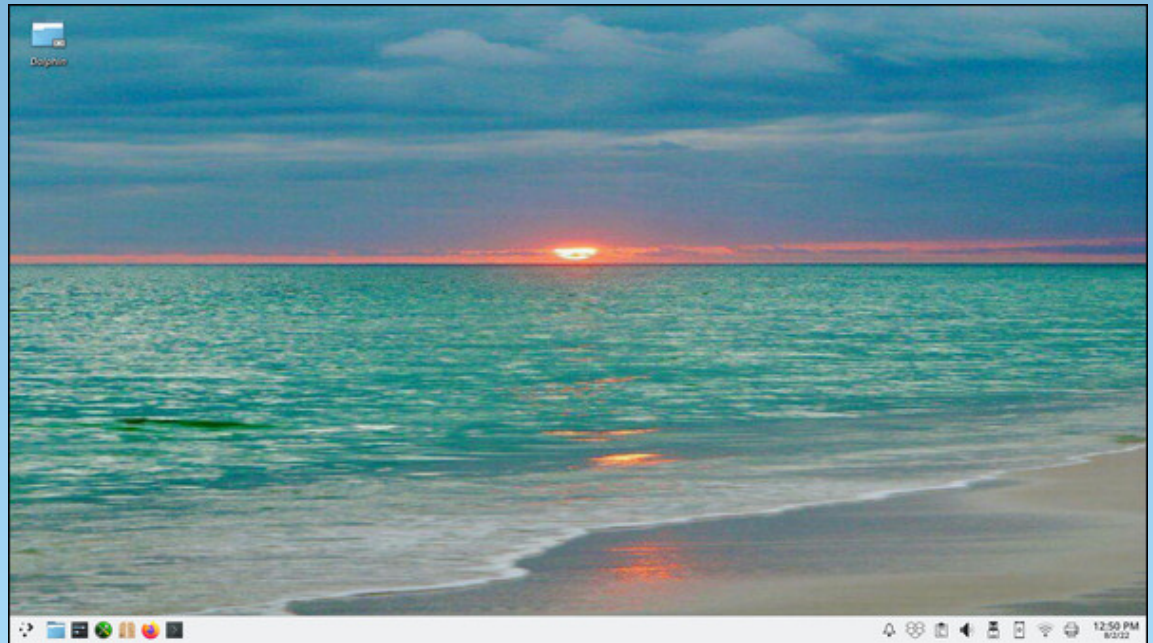
# PCLinuxOS



Like Us On Facebook!  
The PCLinuxOS Magazine  
PCLinuxOS Fan Club



## Screenshot Showcase



*Posted by Texstar, on August 2, 2022, running KDE.*



# PCLinuxOS Recipe Corner



## Chicken & Rice Casserole Foil Packs

Serves 4

### INGREDIENTS:

1 can (10 1/2 oz) condensed cream of chicken soup  
1 1/2 cups unsalted chicken broth  
3 teaspoons Montreal chicken seasoning  
2 cups uncooked instant white rice  
1/2 cup shredded carrot  
1 cup halved, seeded and sliced mini sweet peppers  
4 boneless skinless chicken breasts (6 oz each)  
4 slices cooked bacon, coarsely chopped  
2 green onions, sliced

### DIRECTIONS:

Heat gas or charcoal grill. Cut 4 (18x12-inch) sheets of heavy-duty foil. Spray with cooking spray.

Measure 1/2 cup of the condensed soup, and reserve. In a 4-cup glass measuring cup, mix remaining condensed soup, the chicken broth and 1 teaspoon of the seasoning; beat with whisk to blend. Add instant rice; stir and let stand for about 8 minutes or until most of the liquid is absorbed. Stir in carrots and peppers.

Season chicken with remaining 2 teaspoons seasoning; place on center of each sheet of foil. Dividing evenly, spoon rice and vegetable mixture around each chicken breast. Divide any remaining soaking liquid over the tops of breasts. Spread 2 tablespoons of reserved soup over each breast; evenly top with bacon.

Bring up 2 sides of foil so edges meet. Seal edges, making tight 1/2-inch fold; fold again, allowing space for heat circulation and expansion. Fold other sides to seal.

Place the packs on the grill over medium heat. Cover grill; cook for 10 minutes. Rotate packs 1/2 turn; cook 9 to 10 minutes longer or until juice of chicken is clear when center of thickest part is cut (at least 165F). Remove packs from the grill; cut large X across top of each pack. Carefully fold back foil, and garnish with green onions.

### TIPS:

For a different flavor, substitute golden condensed mushroom soup for cream of chicken soup in this recipe.

To make in a oven, place the packs on a cookie sheet. Bake at 375F 32 to 35 minutes or until the juice of chicken is clear when the center of thickest part is cut (at least 165F).

### NUTRITION:

Calories: 540      Carbs: 55g      Fiber: 2g  
Sodium: 1000mg      Protein: 47g



Linux Docs  
Linux Man Pages



# Online Platforms Should Stop Partnering With Government Agencies To Remove Content

by [David Greene](#), [Paige Collings](#), and [Christoph Schmon](#)  
[Electronic Frontier Foundation](#)  
Reprinted under Creative Commons Attribution [license](#)



Government involvement in content moderation raises serious human rights concerns in every context, and these concerns are further troubling when the involvement originates with law enforcement. We recently filed a [comment](#) with the Meta Oversight Board urging it to treat this issue seriously.

When sites cooperate with government agencies, it leaves the platform inherently biased in favor of the government's favored positions. It gives government entities outsized influence to manipulate content moderation systems for their own political goals—to control public dialogue, suppress dissent, silence political opponents, or blunt social movements. And once such systems are established, it is easy for government—and particularly law enforcement—to use the systems to coerce and pressure platforms to moderate speech they may not otherwise have chosen to moderate.

For example, Vietnam has boasted of its increasing effectiveness in getting Facebook posts removed but has been accused of [targeting dissidents](#) in doing so. Similarly, the Israeli Cyber Unit has boasted of high compliance rates of [up to 90 percent](#) with its takedown requests across all social media platforms. But these requests [unfairly target](#) Palestinian rights activists, news organizations, and civil society, and one such incident prompted the Facebook Oversight Board to

[recommend](#) that Facebook “Formalize a transparent process on how it receives and responds to all government requests for content removal, and ensure that they are included in transparency reporting.”

Issues with government involvement in content moderation were addressed in the newly revised [Santa Clara Principles](#) 2.0 where EFF and other organizations called on social media companies to “recognize the particular risks to users’ rights that result from state involvement in content moderation processes.” The Santa Clara Principles also affirm that “state actors must not exploit or manipulate companies’ content moderation systems to censor dissenters, political opponents, social movements, or any person.”

Specifically, users should be able to access:

- \* Details of any rules or policies, whether applying globally or in certain jurisdictions, which seek to reflect requirements of local laws.
- \* Details of any formal or informal working relationships and/or agreements the company has with state actors when it comes to flagging content or accounts or any other action taken by the company.
- \* Details of the process by which content or accounts flagged by state actors are assessed, whether on the basis of the company’s rules or policies or local laws.
- \* Details of state requests to action posts and accounts.

User access to this information is even more pertinent when social media sites have granted government authorities with “trusted flagger” status to inform the platform about content that is illegal, or which violates its Community Guidelines or Terms of Service. This status has been bestowed on governments even when their own civil liberties record is questionable, thus enabling censorship of discourses that challenge government-imposed narratives.

These concerns about government influence over the content available to users online are even more dire given that the EU’s Digital Services Act (DSA) will soon impose new mechanisms allowing platforms to designate governmental agencies—and potentially law enforcement agencies such as Europol—as trusted flaggers, consequently giving governments priority status to “flag” content for platforms. Although trusted flaggers are only supposed to flag illegal content, the preamble of the DSA encourages platforms to empower trusted flaggers to

## Online Platforms Should Stop Partnering With Government Agencies To Remove Content

act against content incompatible with their terms of service. This opens the door to law enforcement overreach and platforms' over-reliance on law enforcement capacities for the purpose of content moderation.

Moreover, government entities may also simply lack the relevant expertise to effectively flag content on a variety of platform types. This is evident in the United Kingdom where London's Metropolitan Police Service, or the Met, consistently seek to remove drill music from online platforms based on the mistaken, and frankly racist, belief that it is not creative expression at all, but a witness statement to criminal activity. [In a global first](#) for law enforcement, YouTube gave officers from the Met trusted flagger status in 2018 to "achieve a more effective and efficient process for the removal of online content." This pervasive system of content moderation on drill music is governed by the Met's [Project Alpha](#), which involves police officers from gang units operating a database, including drill music videos, and monitoring social media sites for intelligence about criminal activity.

The Met has refuted accusations that Project Alpha suppresses freedom of expression or violates privacy rights. But [reports](#) show that since November 2016, the Met made 579 referrals for the removal of "potentially harmful content" from social media platforms and 522 of these were removed, predominantly from YouTube. A 2022 [report by Vice](#) also found that 1,006 rap videos have been included on the Project Alpha database since 2020, and a heavily redacted [official Met document](#) noted that the project was to carry out "systematic monitoring or profiling on a large scale," with males aged between 15 to 21 the primary focus. Drill lyrics and music videos are not simple or immediate confessions to engagements in criminal activity, yet law enforcement's "[street illiteracy](#)" exacerbates the idea that drill music is an illustration of real-life activities that the artists have themselves seen or done, rather than an artistic expression communicated through culturally-specific language and references that police officers are seldom equipped to decode or understand.

Law enforcement are not experts on music and have a [history of linking it to violence](#). As such, the flags raised by the police to social platforms are completely one-sided, rather than with experts supporting both sides. And it is especially troubling that law enforcement is advancing concerns for gang activity through their partnerships with social media platforms, which is disproportionately targeting youth and communities of color.

Indeed, the removal of a drill music video at the request of unnamed "UK law enforcement" is the very [case](#) the Oversight Board is considering, and on which we commented.

All individuals should be able to share content online without their voices being censored by government authorities because their views are oppositional to that of the powerful. Users should be informed when government agencies have

requested the removal of their content, and companies should disclose any back-channel arrangements they have with government actors—including trusted or other preferred flagger systems—and reveal the specific government actors to whom such privileges and access are granted.



***The PCLinuxOS Magazine***

***Created with Scribus***

***Defending Your Rights***



***In The Digital World***

# Art Project In Gimp 2022

by tuxlink

Recently, in the 'Camera Talk' section of the forum, **TheCrankyZombie** posted a great photo of the full 'Sturgeon' Moon. It had lots of great sharp detail, and most importantly, it was huge in the frame. If you'd like to see and save it, you can find it right here:

<https://www.pclinuxos.com/forum/index.php/topic,152772.msg1363205.html#msg1363205>

Seeing this wonderful shot, and with his generous permission, it gave me an idea for a wallpaper to use on my desktop. I started to think if the moon was in the background, what graphical item would I most like to capture in a silhouette if I was behind the viewfinder of the lens and camera. A bird, a plane, or maybe something natural like trees or animals. This got my inspiration going, so I decided to go look for some silhouettes online. There are plenty of pieces of clip-art available for use online. Steer clear of anything copyrighted, and look for pieces that clearly state for 'free' or 'personal use' only. I decided a wolf howling at the moon would be a nice touch. So after typing in 'free wolf clip-art silhouette' at Google's Image search bar, I found a site with a few silhouettes that would work well for what I had in mind, and saved some.

You can, of course, pick whatever subject you like as a central figure. In fact, I think I'll add a few Pine trees to our project also. So, a quick visit back to [www.Clipart-library.com](http://www.Clipart-library.com) for some pine trees would yield a few nice choices.

Before we start in Gimp, I'd like to encourage you to keep all the elements for this project in one folder.

That way, as you search, save and use, you'll only have to deal with one location. When the project is finished, it's an easy matter to drop and save this folder into your online cloud location as well as your local hard drive, whether it's PCLOSCloud, Dropbox, MEGAsync, Google Drive etc.... All the images used in this project can be downloaded and used from here.

<http://mypics.findmoore.net/?cmd=gallery&u=tuxlink&g=MoonProject2022>

I like listening to music when working in Gimp. Here's links to three 'Moon' themed songs you can listen to while working on this project. Enjoy!

<https://www.youtube.com/watch?v=zUQiUFZ5RDw>

<https://www.youtube.com/watch?v=TQZSQdGJujU>

<https://www.youtube.com/watch?v=4Tr0otuiQuU>

## Let's Get Started!

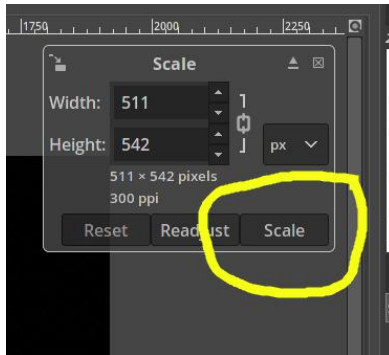
Let's fire up Gimp, and get things started. First, you're going to open the full moon image. After we open the moon shot, then open the file wolf1.png. This file has a white background that we do not need in our silhouette, so, using the Fuzzy Select Tool (or magic wand), click once on the black area only. Now that it's selected, open the 'Edit' menu and choose 'copy' or hit Ctrl+C.

Next, go back to and click on the moon image you opened earlier. Open the 'edit' menu again and this time choose 'paste as new layer'. When the wolf shows up, select the 'Move' tool, then click on it to move it where you'd like it to be (top right).



Next, go back to the project folder and open the file wolf2.png. Do the same thing again, using the Fuzzy Select Tool to select only the black area and copy and paste it into the moon image as well. Now, the first thing we see here is that both wolf images are a tad too big for what I had in mind. So, using the Scale Tool, which is found in the 'Transform' group of tools, select the wolf image over in the 'Layers' palette, then click on the image, grab it at the corner and push it inwards. Resize the image to the size you need, then hit the word 'Scale' to make it happen. Do the same thing for the second wolf image if it's not the correct size. We're going to place the wolves on the moon background loosely for the time being. After we choose and place some pine trees, we will finalize where everything will end up.

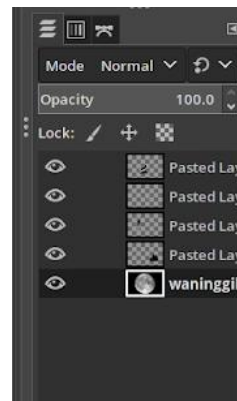
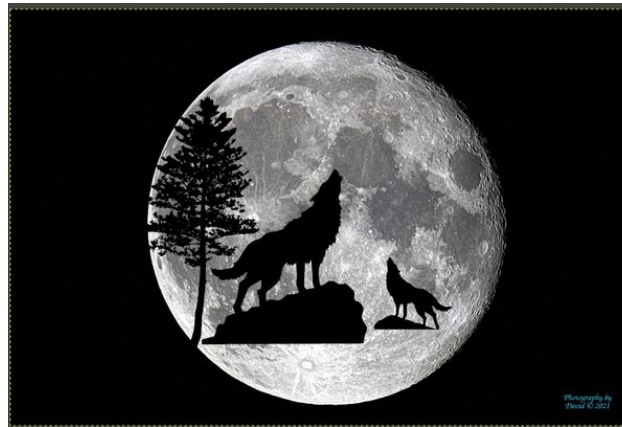




Now, for our trees. Open the file pine1.png and place it on the left or right side of the moon. Clearly this tree is far too big for our needs, so using the 'Scale' tool again, first click on the tree item in the 'Layers' palette, and reduce its size as we did with the wolf images. One good feature to using silhouettes, is that any item may be 'flipped' if the direction it arrived in is not working. Once again, open and choose the pine3.png file, and after sizing it, place it where it looks best.

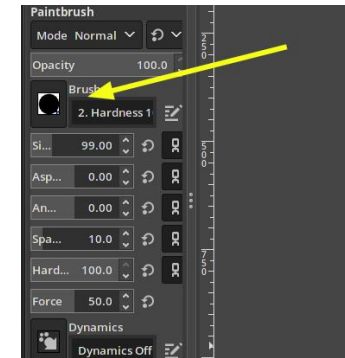


Next, we are going to fill in the remainder of the bottom area that shows the moon. Make sure you have the bottom level layer of the moon only selected before you start. Using the Brush Tool, select a large hard edged brush and start filling in the portion of the moon we don't want to see. You will have the color on the brush selected as black, and you will be painting on the background image of the moon. If you make a mistake, just open the 'Edit' menu and choose 'Undo' as many times as you need.



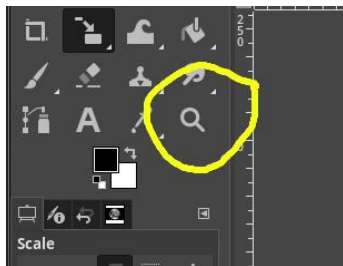
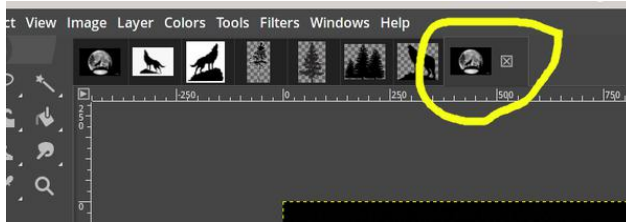
Actually, what I ended up doing was creating a bridge with the Brush Tool. Just use the brush to shape the bridge. The brush has a round shape, so use that to create a bridge under the wolves. It helps here to get in close, so you can make sure to place

the brush as accurately as you can. I like to use the 'Magnify' Tool to draw a box over the area in question, and then you can zoom in and place the brush exactly where you need it.



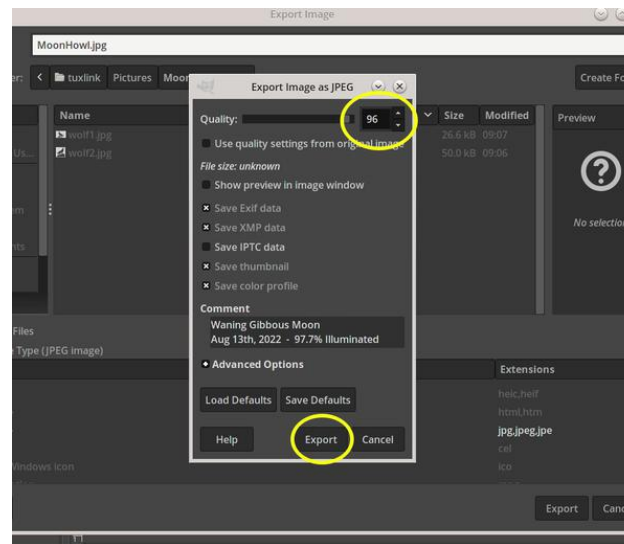
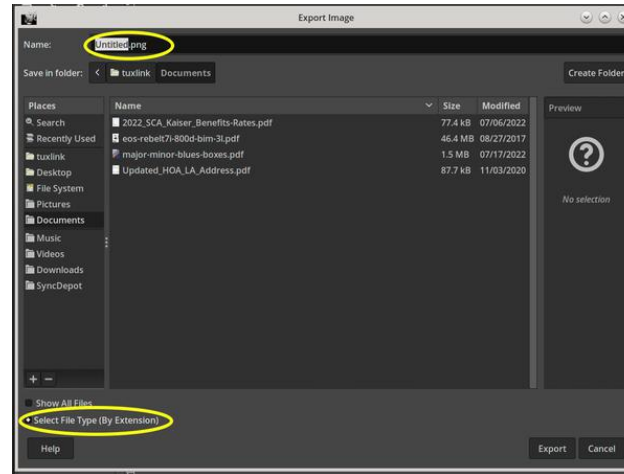
After you've finished and are happy with the final positioning of all elements, make sure to open the File menu and use 'Save As' and save the finished image in Gimp's native format filename.xcf. This way, in the future should you need to revisit this project, you can open it up and add or move the elements around again. Once more, I would suggest you save this file to the project folder. This file is for archival purposes only. The next step will be to make a duplicate, and change the final format extension (next page, top left).

Before you save the final image, the original Moon photo comes with **CrankyZombie's** signature and year on it in light blue on the lower right side.



Whether you want to keep or remove this, the choice is yours, now would be the time to paint over it with the brush. After the next step, if you need to change something, you will have to go back to the .xcf file and do it there. The final step is to open the 'Image' menu and choose 'Flatten Image'. This will lock in all the layers and allow you to save the file in a usable format for use elsewhere.

Open the 'File' menu, choose 'Export As.....' In the dialog box, set the extension to .jpg, and then fill in a unique name for the final file that makes it easy to remember and find. When the next dialog opens,



choose the quality level for the file. Here I chose 96. That should yield a decent quality image for the extension used. (JPG) Now you can display your new creation on your desktop.

A big thank you to **TheCrankyZombie** for allowing use of the original Full Moon image.

The clip-art used in this project came from [www.clipart-library.com](http://www.clipart-library.com).

# PCLinuxOS Users Don't

- Text
- Phone
- Web Surf
- Facebook
- Tweet
- Instagram
- Video
- Take Pictures
- Email
- Chat

*While Driving.*

*Put Down Your  
Phone & Arrive Alive.*



# 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.

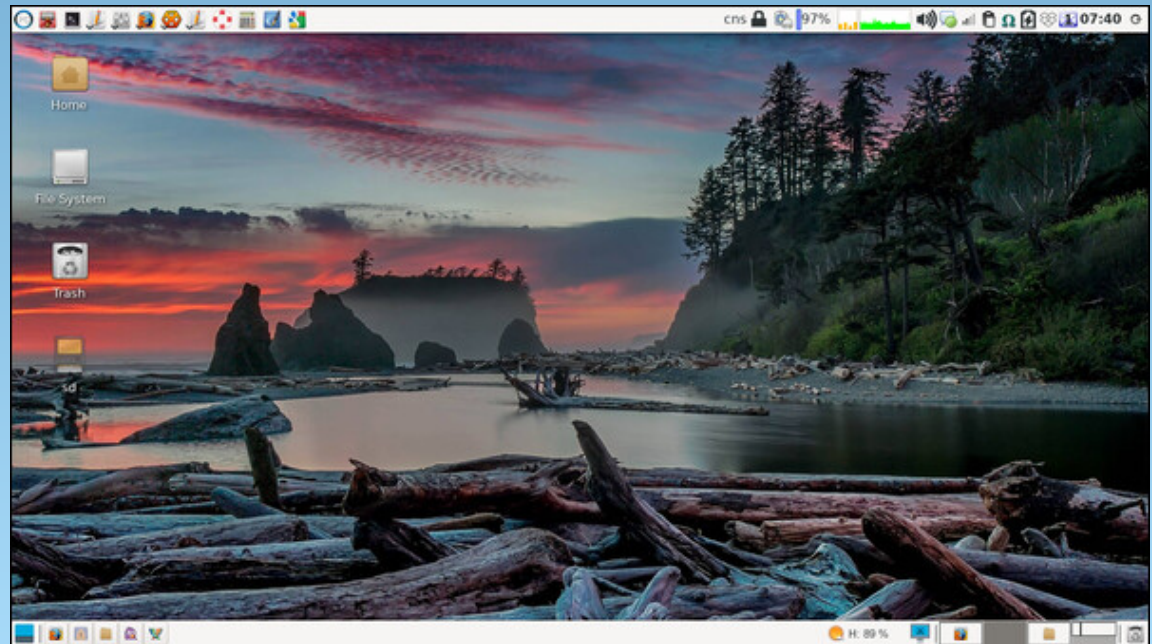


Visit.  
Contribute.  
Build.

The PCLinuxOS  
Knowledge Base

*It Belongs To YOU!*

# Screenshot Showcase



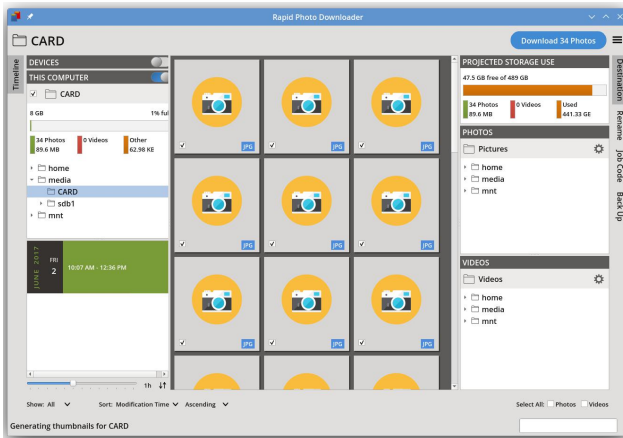
Posted by parnote, on August 11, 2022, running Xfce.



# Repo Review: Rapid Photo Downloader

by CgBoy

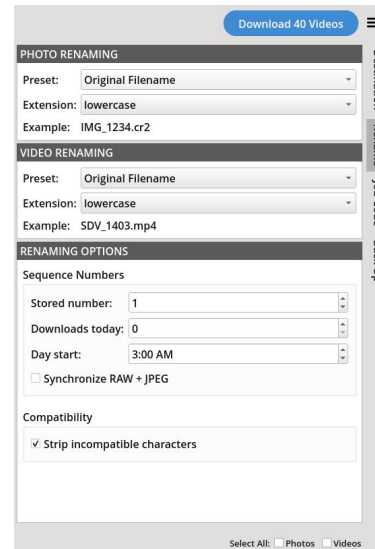
**Rapid Photo Downloader** is a handy tool to help you download and organize photos and videos from your digital cameras. It allows you to easily copy, rename, and backup all of your camera's important data, while supporting most common image and video formats, including RAW photos. Rapid Photo Downloader also has a very nice, easy to use interface.



To begin, you must first select a source to download photos from. You can choose an external media device, such as a camera or card reader, or simply a local folder. Rapid Photo Downloader will show you how much free space is left on the source and destination storage devices.

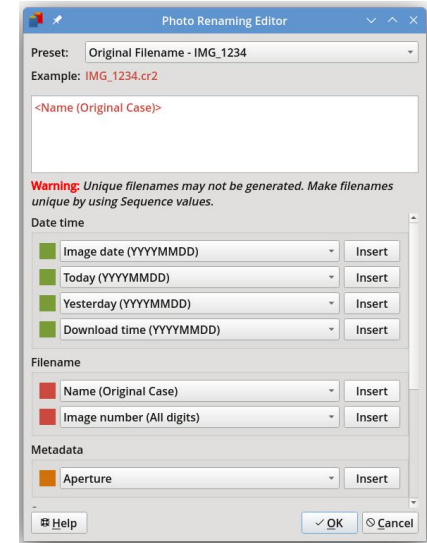
Once you've selected a source, all your images and videos will appear as thumbnails in the main screen, allowing you to choose and sort which ones you want to download. To the left is the timeline, which allows you to find photos based on the date you've taken them and how much time has elapsed

between each group of photos. Once you are satisfied with all the options, you can choose a download destination. Photos and videos can be downloaded to separate destinations.



Rapid Photo Downloader lets you rename all your photos and videos when they are downloaded. You can choose from a variety of filename presets, such as date-time and image number, date and number of image downloads, date-time and job code, image resolution, or you can create your own custom file naming scheme.

Job codes can be created and used as labels to help you organize your photos and videos. For example, you can create a job code called *Wedding* and apply it to one group of photos to help differentiate them from another group with the job code *Birthday*. You can then use the job codes to control the file and directory names when downloading photos (right, top).



Rapid Photo Downloader also gives you the option to back up photos and videos to another location as they are downloaded. You can choose a custom location, or simply let Rapid Photo Downloader automatically detect and use any storage devices connected (Flash drives, external hard drives, etc). When you're finally ready, just hit the big Download button to start downloading your photos.

## Summary

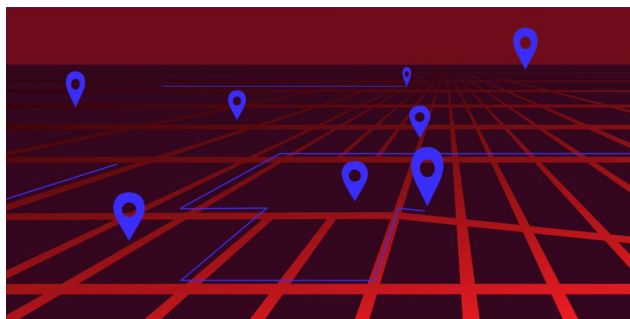
When using Rapid Photo Downloader, I did encounter some issues, such as thumbnails not always generating properly, as well as a few other minor problems, but I am unsure if these are program bugs, or some sort of Python issues. All in all, however, Rapid Photo Downloader is still a very useful and very easy to use utility for any photographer.

# Bad Data “For Good”: How Data Brokers Try To Hide Behind Academic Research

by [Gennie Gebhart](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons Attribution license



When data broker SafeGraph [got caught selling location information on Planned Parenthood visitors](#), it had a public relations trick up its sleeve. After the company agreed to [remove family planning center data](#) from its platforms in response to public outcry, CEO Auren Hoffman tried to flip the narrative: he [claimed](#) that his company’s harvesting and sharing of sensitive data was, in fact, an engine for beneficial [research](#) on abortion access. He even argued that SafeGraph’s post-scandal removal of the clinic data was the real problem: “Once we decided to take it down, we had hundreds of researchers complain to us about...taking that data away from them.” Of course, when pressed, Hoffman could not name any individual researchers or institutions.

SafeGraph is not alone among location data brokers in trying to “research wash” its privacy-invasive business model and data through academic work. Other shady actors like [Veraset](#), [Cuebiq](#), [Spectus](#), and [X-Mode](#) also operate so-called “data for good” programs with academics, and have seized on the

pandemic to expand them. These data brokers provide location data to academic researchers across disciplines, with resulting publications appearing in peer-reviewed venues [as prestigious as Nature](#) and the [Proceedings of the National Academy of Sciences](#). These companies’ data is so widely used in human mobility research—from epidemic forecasting and emergency response to urban planning and business development—that the literature has progressed to meta-studies [comparing, for example, Spectus, X-Mode, and Veraset datasets](#).

Data brokers variously claim to be bringing “transparency” to tech or “[democratizing access to data](#).” But these data sharing programs are nothing more than data brokers’ attempts to control the narrative around their [unpopular](#) and [non-consensual business practices](#). Critical academic research must not become reliant on profit-driven data pipelines that endanger the safety, privacy, and economic opportunities of millions of people without any meaningful consent.

## Data Brokers Do Not Provide Opt-In, Anonymous Data

Location data brokers do not come close to meeting human subjects research standards. This starts with the fact that meaningful opt-in consent is consistently missing from their business practices. In fact, Google concluded that SafeGraph’s practices were so out of line that it [banned any apps using the company’s code](#) from its Play Store, and both Apple and Google [banned X-Mode](#) from their respective app stores.

Data brokers frequently argue that the data they collect is “opt-in” because a user has agreed to

share it with an app—even though the overwhelming majority of users have no idea that it’s being sold on the side to data brokers who in turn sell to businesses, [governments](#), and others. Technically, it is true that users have to opt in to sharing location data with, say, a [weather app](#) before it will give them localized forecasts. But no reasonable person believes that this constitutes blanket consent for the laundry list of data sharing, selling, and analysis that any number of shadowy third parties are conducting in the background.

No privacy-preserving aggregation protocols can justify collecting location data from people without their consent.

On top of being collected and shared without consent, the data feeding into data brokers’ products can easily be linked to identifiable people. The companies claim their data is anonymized, but there’s simply no such thing as anonymous location data. Information about where a person has been is itself enough to re-identify them: one [widely cited study from 2013](#) found that researchers could uniquely characterize 50% of people using only two [randomly](#) chosen time and location data points. Data brokers today collect sensitive user data from a wide variety of sources, including hidden tracking in the background of mobile apps. While techniques vary and are often hidden behind layers of non-disclosure agreements (or NDAs), the resulting raw data they collect and process is based on sensitive, individual location traces.

[Aggregating location data](#) can sometimes preserve individual privacy, given appropriate parameters that take into account the number of people represented in the data set and its granularity. But no privacy-preserving aggregation protocols can justify the initial collection of location data from people without

## Bad Data “For Good”: How Data Brokers Try To Hide Behind Academic Research

their voluntary, meaningful opt-in consent, especially when that location data is then exploited for profit and PR spin.

Data brokers' products are notoriously [easy to re-identify](#), especially when combined with other data sets. And combining datasets is exactly what some academic studies are doing. Published studies have combined data broker location datasets [with Census data](#), [real-time Google Maps traffic estimates](#), and [local household surveys and state Department of Transportation data](#). While researchers appear to be simply building the most reliable and comprehensive possible datasets for their work, this kind of merging is also the first step someone would take if they wanted to re-identify the data.

### NDA's, NDAs, NDAs

Data brokers are not good sources of information about data brokers, and researchers should be suspicious of any claims they make about the data they provide. As Cracked Labs researcher [Wolfie Christl](#) puts it, what data brokers have to offer is “potentially flawed, biased, untrustworthy, or even fraudulent.”

Some researchers incorrectly describe the data they receive from data brokers. For example, one paper describes SafeGraph data as “[anonymized](#) human mobility data” or “foot traffic data from [opt-in](#) smartphone GPS tracking.” Another describes Spectus as providing “anonymous, privacy-compliant location data” with an “[ironclad](#) privacy framework.” Again, this location data is not opt-in, not anonymized, and not privacy-compliant.

Other researchers make internally contradictory claims about location data. One Nature paper characterizes Veraset's location data as achieving the impossible feat of being [both “fine-grained” and “anonymous.”](#) This paper further states it used such specific data points as “anonymized device IDs” and

“the timestamps, and precise geographical coordinates of dwelling points” where a device spends more than 5 minutes. Such fine-grained data cannot be anonymous.

All of this should be a red flag for Institutional Review Boards, which need visibility into whether data brokers actually obtain consent.

A Veraset Data Access Agreement [obtained by EFF](#) includes a Publicity Clause, giving Veraset control over how its partners may disclose Veraset's involvement in publications. This includes Veraset's prerogative to approve language or remain anonymous as the data source. While the Veraset Agreement we've seen was with a municipal government, its suggested language [appears in multiple academic publications](#), which suggests a similar agreement may be in play with academics.

A similar pattern appears in papers using X-Mode data: some use [nearly verbatim](#) language to describe the company. They even claim its NDA is a good thing for privacy and security, stating: “All researchers processed and analyzed the data under a non-disclosure agreement and were obligated to not share data further and not to attempt to re-identify data.” But those same NDAs prevent academics, journalists, and others in civil society from understanding data brokers' business practices, or identifying the web of data aggregators, ad tech exchanges, and mobile apps that their data stores are built on.

All of this should be a red flag for Institutional Review Boards, which review proposed human subjects research and need visibility into whether and how data brokers and their partners actually obtain consent from users. Likewise, academics themselves need to be able to confirm the integrity and provenance of the data on which their work relies.



### From Insurance Against Bad Press to Accountable Transparency

Data sharing programs with academics are only the tip of the iceberg. To paper over [the dangerous role they play](#) in the online data ecosystem, data brokers forge relationships not only with academic institutions and researchers, but also with [government authorities](#), [journalists](#) and [reporters](#), and [non-profit organizations](#).

The question of how to balance data transparency with user privacy is [not a new one](#), and it can't be left to the Veraset's and X-Mode's of the world to answer. Academic data sharing programs will continue to function as disingenuous PR operations until companies are subjected to data privacy and transparency requirements. While SafeGraph claims its data could pave the way for impactful research in abortion access, the fact remains that the very same data puts actual abortion seekers, providers, and advocates in danger, [especially in the wake of Dobbs](#). The sensitive data location data brokers deal in should only be collected and used with specific, informed consent, and subjects must have the right to withdraw that consent at any time. No such consent currently exists.

We need [comprehensive federal consumer data privacy legislation](#) to enforce these standards, with a [private right of action](#) to empower ordinary people to bring their own lawsuits against data brokers who violate their privacy rights. Moreover, we must pull back the NDAs to allow research investigating these data brokers themselves: their business practices, their partners, how their data can be abused, and how to protect the people whom data brokers are putting in harm's way.



# Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

by Paul Arnote (parnote)

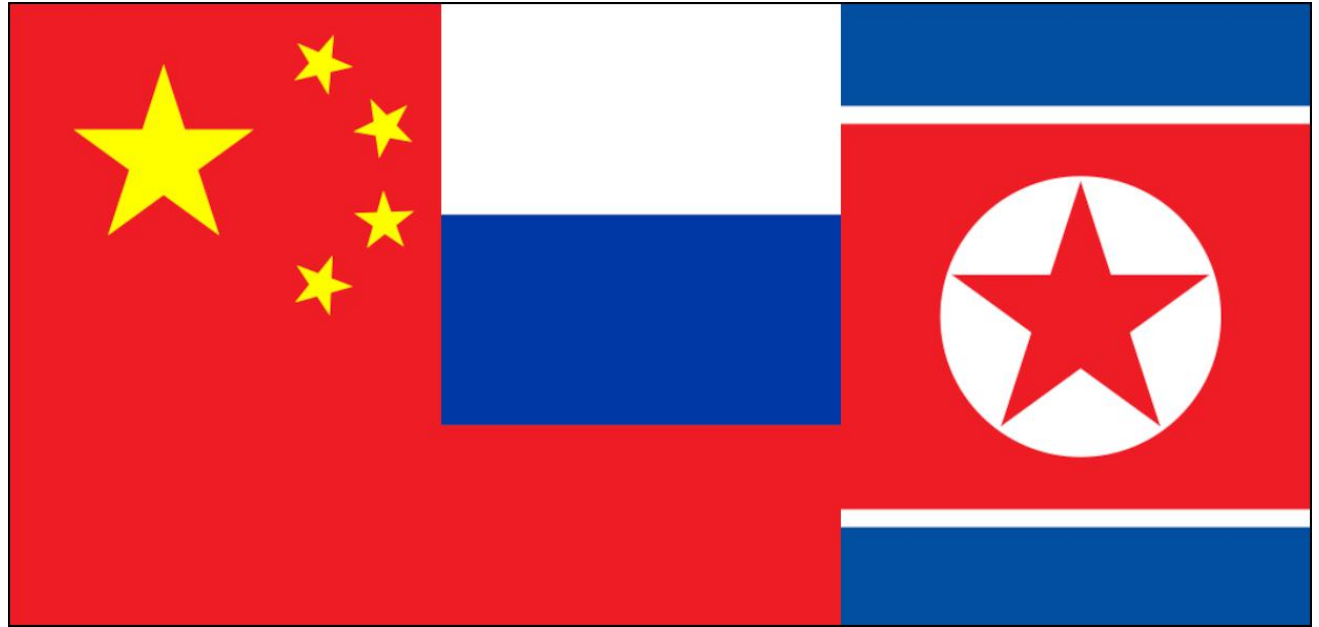
## Assault On Your Privacy: Monthly Update

The cybersecurity firm WithSecure has [identified](#) a **Facebook malware campaign**, dubbed “DUCKTAIL,” that targets individuals and organizations that operate on Facebook’s Business and Ads platform. The malware steals browser cookies to gain access to the accounts and the private information associated with those accounts. You can read a more detailed accounting of the malware from the [article](#) on TechRepublic.

**Millions of Android devices are infected with “wallet-draining malware,”** according to an [article](#) on TechRadar Pro. The article identifies 28 Google Play Store apps. All but three of the apps have been removed from the Google Play Store, according to the TechRadar Pro article. Another [article](#) on Komando.com listed the number of infected apps as 36 in the Google Play Store.

Another 17 Android apps have been caught **compromising users’ devices with banking malware called DawDropper**, [according](#) to researchers at Trend Micro. The malware masqueraded as productivity and utility apps.

Don’t underestimate the importance of keeping your system up-to-date. Whether you’re responsible for the maintenance of 1,000 corporate computers on a network, or just your private home network, the job is the same and requires the same amount of diligence. According to the Palo Alto Networks Unit 42 Incident Response [report](#), **hackers start looking for potential targets within about 15 minutes of a CVE (bug) being reported.**



According to an [article](#) on The Hacker News, **North Korean hackers have deployed a malicious browser extension for Chromium-based browsers** (Chromium, Google Chrome, Microsoft Edge, Brave, Opera, etc.) **capable of stealing email content from Gmail and AOL.** Discovered by cybersecurity firm [Velocity](#), the malware is called SharpTongue, and it is capable of singling out individuals working for organizations in the U.S., Europe and South Korea who work on topics involving North Korea, nuclear issues, weapons systems, and other matters of strategic interest to North Korea.

Apple iOS users didn’t escape the past month unscathed. According to an [article](#) on Lifehacker, **security researcher Alex Kleber discovered seven malware apps hiding in plain sight.** While initially appearing to be by separate publishers,

Kleber discovered that the malware apps were all created by a single group of hackers in China.

Here’s a BIG oops! With the **Google Pixel 6a** hitting stores, **reports have emerged about ANYONE’S fingerprint being able to unlock the phone ...** not just the user who registered their fingerprint, according to an [article](#) on 9 to 5 Google.

Still think all of those so-called “smart devices” are worth the trouble or a great idea? Well, [here’s](#) an excellent **exposé from Lifehacker about how all of these “smart devices” and IoT (which I’ve always called I(di)oT) devices sacrifice your privacy all in the name of convenience.** This is what I’ve been saying all along. Remember that there is a literal GOLDMINE available in the reselling of your data, so it’s going to be difficult (without legal or legislative restraints) to limit ANY company from profiting off of

## Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

your data by selling and reselling your data to other “interested” parties ... whose only interest is in serving up advertising and other tracking information. Even metadata or anonymized data, given enough of it, can paint a pretty accurate picture of a user from bits of innocent-looking data. In aggregate, it's not so innocent. THIS article deserves your attention, since the markets are now inundated by smart appliances, smart bulbs, smart thermostats, smart speakers, etc. (when I recently purchased a new thermostat for my house, the “non-smart” thermostats were buried on the retailer's website, and harder to find than they should have been). Scary, scary times ahead concerning privacy!

According to an [article](#) on BleepingComputer, **another batch of 35 malware apps has been found in the Google Play Store.** This latest batch of malware has been installed more than 2,000,000 times.

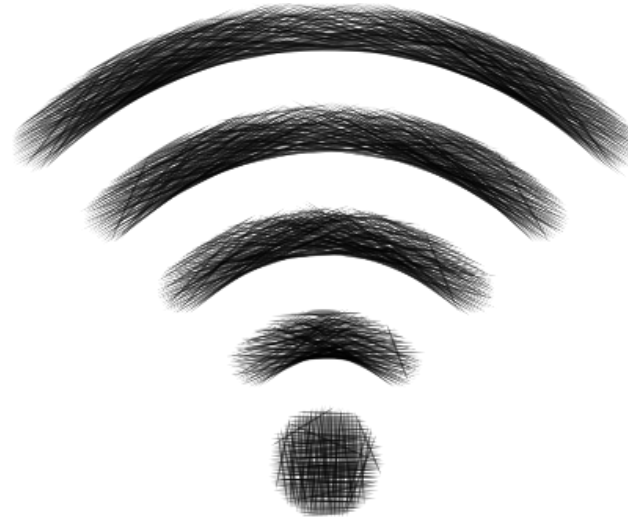
Research from cybersecurity provider [Kaspersky](#) found nearly **7 million users being affected by unwanted software disguised as browser add-ons**, with many being found on Google Chrome. As reported, 4.3 million unique users were attacked by adware sneaking their way onto systems, while over 2.6 million users were affected by malware, according to an [article](#) from Laptop Mag.

**“Bad actors” have been discovered creating false Google Ads** in an effort to deliver malware to your computer, according to an [article](#) from Lifehacker. The “malvertising” disguises itself as a bona fide Google Ad to lure unsuspecting/less savvy users to a fake version of the site that's being searched for. We all knew ads were bad, but now they are even worse.

If you haven't changed to Bitwarden to help manage your online passwords, you may want to after hearing this. **LastPass, one of the world's largest password managers, has confirmed** on a blog post **that it has been hacked**, according to an [article](#) on Forbes. LastPass, which recently switched

from a free service to a fee-based subscription service, has about 25 **million** users. While user data was never compromised, the hackers did gain access to some proprietary LastPass technical information, and gained access to some portions of source code.

### Mystery Solved: What Does Wi-Fi Stand For?



Here's a debate that has raged for years: what does Wi-Fi actually stand for? If you (like many others) say “wireless fidelity,” you would actually be ... wrong.

It's actually a trick question. The name “Wi-Fi” actually doesn't mean anything. Instead, it's a meaningless marketing term.

Writes Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name “Wi-Fi” in a 2005 BoingBoing [article](#) by Cory Doctorow:

*Wi-Fi doesn't stand for anything.*

*It is not an acronym. There is no meaning.*

*Wi-Fi and the ying yang style logo were invented by Interbrand. We (the founding members of the Wireless Ethernet Compatibility Alliance, now called the Wi-Fi Alliance) hired Interbrand to come up with the name and logo that we could use for our interoperability seal and marketing efforts. We needed something that was a little catchier than “IEEE 802.11b Direct Sequence”. Interbrand created “Prozac”, “Compaq” “oneworld”, “Imation” and many other brand names that you have heard of. They even created the company name “Vivato”.*

*The only reason that you hear anything about “Wireless Fidelity” is some of my colleagues in the group were afraid. They didn't understand branding or marketing. They could not imagine using the name “Wi-Fi” without having some sort of literal explanation. So we compromised and agreed to include the tag line “The Standard for Wireless Fidelity” along with the name. This was a mistake and only served to confuse people and dilute the brand. For the first year or so( circa 2000) , this would appear in all of our communications. I still have a hat and a couple of golf shirts with the tag line. Later, when Wi-Fi was becoming more successful and we got some marketing and business people from larger companies on the board, the alliance dropped the tag-line.*

*This tag line was invented after the fact. After we chose the name Wi-Fi from a list of 10 names that Interbrand proposed. The tag line was invented by the initial six member board and it does not mean anything either. If you decompose the tag line, it falls apart very quickly. “The Standard”? The Wi-Fi Alliance has always been very careful to stay out of inventing standards. The standard of interest is IEEE 802.11. The Wi-Fi Alliance focuses on interoperability certification and branding. It does not invent standards. It does not compete with IEEE. It complements their efforts. So Wi-Fi could never be a standard. And “Wireless Fidelity” – what does that mean? Nothing. It was a clumsy attempt to come up with two words that matched Wi and Fi. That's it.*

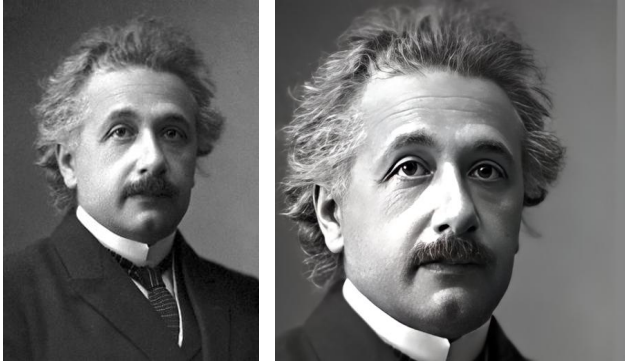
*So we were smart to hire Interbrand to come up with the name and logo. We were dumb to confuse and water down their efforts by adding the meaningless tag line. Please*



## Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

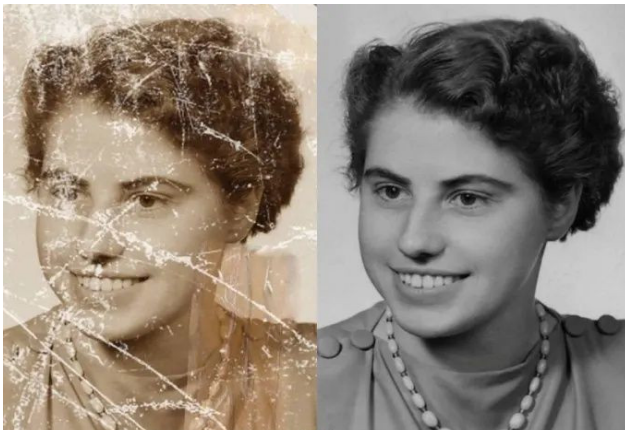
*help reinforce the good work that we did and forget the tag line.*

### New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds



A new and open source AI model can now “fix” most old photos in just seconds ... for free! With the new GFP-GAN (Generative Facial Prior-Generative Adversarial Network) tool, old photos can be fixed to provide a much more lifelike appearance.

Not only does the new process work for old photographs where the colors are faded, but it can also take a black and white photo and colorize it. The real “magic” of the tool comes in the reconstruction of damaged areas of a photograph.



Can you imagine trying to repair the above image on the left? The new AI tool created the image on the right in just a matter of seconds. It would literally take HOURS to try to repair all of that damage, and the results would not look as good as the results from the AI tool.

If you want to read all of the nitty-gritty about the new AI tool, head on over to Louis Bouchard's home [page](#) where he describes the process. He has also created a YouTube video about the process, which you can view [here](#). If you want to take a DEEP dive into the internals of how this whole process works, you can check out the [PDF](#) study paper. Finally, don't hesitate to check out the GitHub [page](#), where you can find the software libraries and a working demo for this new tool.

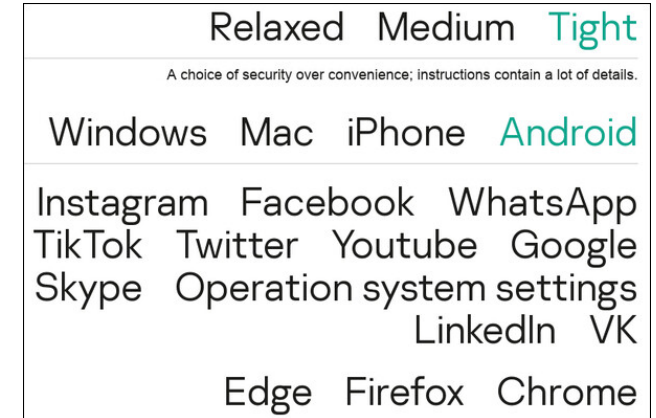
### Concerned About How To Protect Your Online Privacy? Read On...



Increasingly, users of online services are concerned about their privacy. And, gauging by the ongoing monthly section of this article highlighting assaults on user privacy, users have good reason to be concerned. According to a TechRepublic [article](#), 85% of Android users are concerned about privacy ... or their ongoing lack thereof.

What's worse is that it's like trying to navigate through a virtual minefield, with all of the different apps with different privacy settings, and with each app's privacy settings in different places and covering/offering different levels of protection.

Kaspersky, one of the leaders in antivirus/anti-malware software, has an online privacy checker [site](#). While it doesn't cover Linux, it does cover Windows, MacOS, iOS and Android ... and lots of Linux users have/use those platforms as well.



As you can see in the screenshot image above, users can choose between relaxed, medium or tight security. The “relaxed” setting prioritizes convenience over security, while the “medium” setting tries to strike a balance between convenience and security. Selecting the “tight” setting emphasizes security over convenience, and comes with LOTS of detailed instructions on how to achieve a level of heightened security.

Users then choose which app(s) they are wanting greater security/privacy with, and then the browser they use most.

What I find most ironic from looking at the list of apps that it helps users manage privacy settings on, is that most of the apps listed are literal sieves when it comes to user privacy in the first place. Couple that with Edge or Chrome, and you have a privacy nightmare that's nearly impossible to navigate successfully.

Still, the site offers a roadmap to many privacy settings that are most often obfuscated or obscured by being buried so deeply. The ultimate solution is to

## Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

avoid using these apps altogether, if possible. But, barring that abstinence, the recommendations from the Kaspersky Online Privacy Checker is a good place to start.

As a bonus, Kaspersky also offers an online password checker further down on the page. With it, you can see how many years it might take a supercomputer to break/hack your secure password. You are using a secure password, right? You aren't using the same password on multiple sites, right? Ahmm!

### Two Astrophotographers Team Up, Create Highest Resolution Photo Of Moon Ever

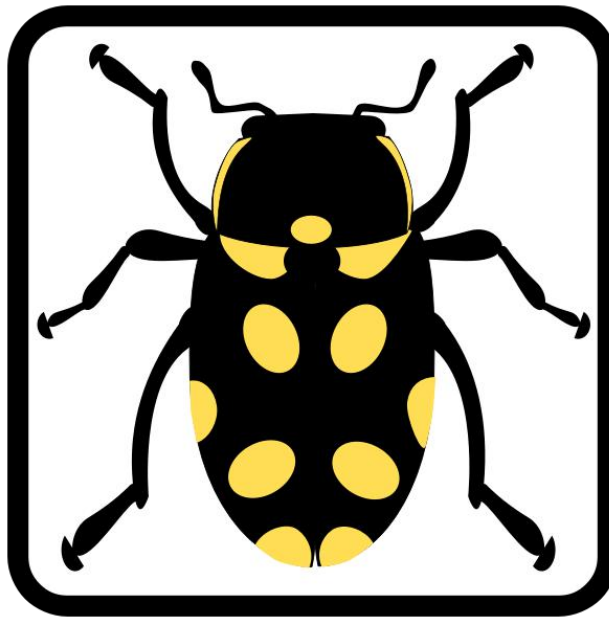


Two astrophotographers teamed up to create two of the most detailed images ever taken of the moon, according to an [article](#) from NPR (check out the New York Post [article](#) for even more information). It took over 500 images to capture the subtle colors of the moon, and was assembled using a technique called photo stitching. The black and white image was

made from 200,000 separate images, also assembled using photo stitching. That effectively made the black and white image a 174 megapixel image, with the most astounding detail ever recorded in an image of the moon.

The image above is called “The Hunt For Artemis,” paying homage to the upcoming Artemis I mission. That mission will launch three test dummies into orbit around the moon to test out NASA’s new moon launch vehicle, before returning to Earth for a splashdown in the Pacific Ocean. Artemis III is scheduled for the first live crew launched to the moon since Apollo 17 in 1972, and should occur in 2025.

### New Vulnerability Found In Linux Kernel, Previously Unknown



**DirtyCred** is a kernel exploitation concept that swaps unprivileged [kernel credentials](#) with privileged ones to escalate privilege. Instead of overwriting any critical data fields on kernel heap, DirtyCred abuses

the heap memory reuse mechanism to get privileged. Although the concept is simple, it is effective, reports the GitHub [page](#) about the vulnerability.

From the [description](#) of the talk presented by researchers at the 2022 Blackhat hacking conference:

*Dirty pipe is the name given to the CVE-2022-0847 vulnerability, present in Linux kernel versions 5.8 and later. It is considered a very serious vulnerability found in the Linux kernel recently partially because it gives a bad actor the ability to escalate privilege but more importantly, its exploitation has no headache in dealing with kernel address randomization and pointer integrity check. With this capability, the exploit built on top of the dirty pipe could be easily used for all versions of kernel affected without even modification.*

*While dirty pipe is powerful, its exploitability is closely tied to the capability of the CVE-2022-0847 vulnerability which abuses the Linux kernel pipe mechanism to inject data to arbitrary files. For other vulnerabilities without such a pipe-abusive power, the exploitation is still hard to follow the dirty pipe journey and thus brings the same level of security implication.*

*In this talk, we present a novel exploitation method pushing the dirty pipe to the next level. To be specific, given a vulnerability with a double-free ability, we will demonstrate that our exploitation method could obtain the dirty-pipe-like ability to overwrite an arbitrary file to escalate privilege. Exploits utilizing our method inherit the advantage of the dirty pipe that the code would work on any version of the kernel affected without modification. We argue that our new exploitation method is not only more general than the dirty pipe but also more powerful. First, rather than tying to a specific vulnerability, this exploitation method allows any vulnerabilities with double-free ability to demonstrate dirty-pipe-like ability. Second, while it is like the dirty pipe that could bypass all the kernel protections, our exploitation method could even demonstrate the ability to escape the container actively that dirty pipe is not capable of.*

## Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

*Along with this talk, we will demonstrate how our exploitation method works using real world vulnerabilities. Specifically, we will demonstrate privilege escalation on Linux and Android. Last but not least, we will demonstrate how to achieve container escape on CentOS. We will release our exploitation details and all of our exploits demonstrated in this talk. To the best of our knowledge, our exploitation is the first general method that helps develop a universal exploit to different versions of kernel and different architectures. It greatly unloads the burden of exploit migration across versions and architectures. Since our exploitation is general and powerful, it also imposes a great challenge to the existing kernel defense architecture.*

The vulnerability exists for all major distros, and has been compared to the previous Dirty Pipe vulnerability, which has been patched. As of the time of this article, the new vulnerability has not yet been patched. It can allow local users to gain root privileges.

### Messin' With Mother Nature: The Return Of The Woolly Mammoth



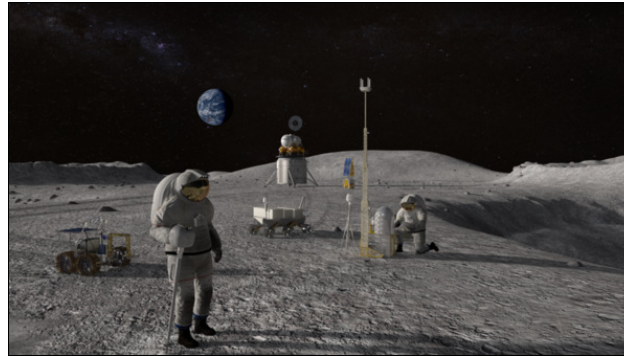
According to an [article](#) from The Independent, a Texas startup is attempting to use genetic engineering to bring back the extinct woolly mammoth. As you can imagine, this attempt has sparked all kinds of ethical discussions.

Woolly mammoths last walked the Earth with humans over 3900 years ago, going extinct just after the last ice age. Since then, no human has ever laid eyes on a living mammal of such size. Then, woolly mammoths were a valuable food source for humans.

The company is touting how good woolly mammoths might be for a healthier planet. The animal's massive weight will help keep the permafrost compacted, which helps to prevent it from melting, and thus keeping greenhouse gasses sequestered in the frozen mix.

Of course, others are asking other questions. Since woolly mammoths provided a significant food source for humans, will we find woolly mammoth meat making its way into our grocery stores?

### NASA Awards Next-Generation Spaceflight Computing Processor Contract



NASA's Jet Propulsion Laboratory has selected Microchip Technology Inc. to develop a high-performance spaceflight computing processor that will support future space missions.

NASA's Jet Propulsion Laboratory has selected Microchip Technology Inc. to develop a high-performance spaceflight computing processor that will support future space missions. Credits: NASA

NASA's Jet Propulsion Laboratory in Southern California has selected Microchip Technology Inc. of Chandler, Arizona, to develop a High-Performance Spaceflight Computing (HPSC) processor that will provide at least 100 times the computational capacity of current spaceflight computers. This key capability would advance all types of future space

missions, from planetary exploration to lunar and Mars surface missions.

"This cutting-edge spaceflight processor will have a tremendous impact on our future space missions and even technologies here on Earth," said Niki Werkheiser, director of technology maturation within the Space Technology Mission Directorate at NASA Headquarters in Washington. "This effort will amplify existing spacecraft capabilities and enable new ones and could ultimately be used by virtually every future space mission, all benefiting from more capable flight computing."

Microchip will architect, design, and deliver the HPSC processor over three years, with the goal of employing the processor on future lunar and planetary exploration missions. Microchip's processor architecture will significantly improve the overall computing efficiency for these missions by enabling computing power to be scalable, based on mission needs. The design also will be more reliable and have a higher fault tolerance. The processor will enable spacecraft computers to perform calculations up to 100 times faster than today's state-of-the-art space computers. As part of NASA's ongoing commercial partnership efforts, the work will take place under a \$50 million firm-fixed-price contract, with Microchip contributing significant research and development costs to complete the project.

"We are pleased that NASA selected Microchip as its partner to develop the next-generation space-qualified compute processor platform," said Babak Samimi, corporate vice president for Microchip's Communications business unit. "We are making a joint investment with NASA on a new trusted and transformative computer platform. It will deliver comprehensive Ethernet networking, advanced artificial intelligence/machine learning processing and connectivity support while offering unprecedented performance gain, fault-tolerance, and security architecture at low power consumption. We will foster an industry-wide ecosystem of single board computer partners anchored on the HPSC

## Short Topix: New Free, Open Source AI Tool Can Fix Most Old Photos In Seconds

processor and Microchip's complementary space-qualified total system solutions to benefit a new generation of mission-critical edge compute designs optimized for size, weight, and power."

Current space-qualified computing technology is designed to address the most computationally-intensive part of a mission – a practice that leads to over-designing and inefficient use of computing power. For example, a Mars surface mission demands high-speed data movement and intense calculation during the planetary landing sequence. However, routine mobility and science operations require fewer calculations and tasks per second. Microchip's new processor architecture offers the flexibility for the processing power to ebb and flow depending on current operational requirements. Certain processing functions can also be turned off when not in use, reducing power consumption. This capability will save a large amount of energy and improve overall computing efficiency for space missions.

"Our current spaceflight computers were developed almost 30 years ago," said Wesley Powell, NASA's principal technologist for advanced avionics. "While they have served past missions well, future NASA missions demand significantly increased onboard computing capabilities and reliability. The new computing processor will provide the advances required in performance, fault tolerance, and flexibility to meet these future mission needs."

Microchip's HPSC processor may be useful to other government agencies and applicable to other types of future space missions to explore our solar system and beyond, from Earth science operations to Mars exploration and human lunar missions. The processor could potentially be used for commercial systems on Earth that require similar mission critical edge computing needs as space missions and are able to safely continue operations if one component of the system fails. These potential applications include industrial automation, edge computing, time-sensitive ethernet data transmission, artificial

intelligence, and even Internet of Things gateways, which bridge various communication technologies.

In 2021, NASA solicited proposals for a trade study for an advanced radiation-hardened computing chip with the intention of selecting one vendor for development. This contract is part of NASA's [High-Performance Space Computing](#) project. HPSC is led by the agency's Space Technology Mission Directorate's [Game Changing Development program](#) with support from the Science Mission Directorate. The project is led by JPL, a division of Caltech.

### PCLinuxOS Magazine Short Topix Roundup



**Linux creator Linus Torvalds has announced the first release candidate for the Linux kernel version 6.0**, but he says the major number change doesn't signify anything especially different about this release, according to an [article](#) on ZDNet.

**Have you ever dropped your cell phone into water?** If so, you may have thrown out the very thing that could **possibly** save your phone,

according to an [article](#) from ZDNet. The article recommends saving those "non-edible" chiclet bags of silica gel that come in pairs of new shoes, electronic devices, and many other things. Place them and your drenched phone in an airtight container ... then wait a few days. They might just resurrect your drenched device(s) and buy you some time. Buy you some time? Yes, because you will still have to deal with the corrosion from the liquid you dropped your device(s) into, but that will be somewhere down the road.

It should be common knowledge by now, **but Google uses a homegrown version of Linux on its thousands of workstations at its offices. Known as gLinux**, it's based on Debian, which has longer LTS support than the initial Goobuntu version (can you guess what that was based on?) that they started with. Ubuntu's LTS support is pretty much limited to two years. With the thousands of computers to keep up-to-date, that would make updating a full-time job before you have to start all over again. If you want to know more about gLinux ... the version of Linux you will never be able to use "in the wild," check out the [article](#) on Computerworld.

**The internet has been built on the back of TCP connections.** TCP stands for Transmission Control Protocol, and has been entrenched as the standard for the past 40 years. But according to an [article](#) from The Register, while cutting edge for its time at the time of its introduction, TCP doesn't work as well for modern data centers. For that, [Homa](#) was conceived (PDF). Homa has the potential to speed things up by 100X over the speed of TCP.

**The James Webb Space Telescope keeps breaking its own records**, according to an [article](#) on Space.com. Sifting through the data returned thus far, astronomers are now able to see distant galaxies as they existed 200 million years after the Big Bang. Previously, they could only see galaxies as far back as 480 million years after the Big Bang.

NASA's DART mission will purposefully crash an unmanned space probe into an asteroid (Dimorphos) as a demonstration of its plan to divert or otherwise change the course of an asteroid that might be on an Earth trajectory, according to an [article](#) on LiveMINT. DART stands for Double Asteroid Redirection Test. The demonstration will take place on September 26, 2022, and will be aired on NASA TV and the space agency's website.



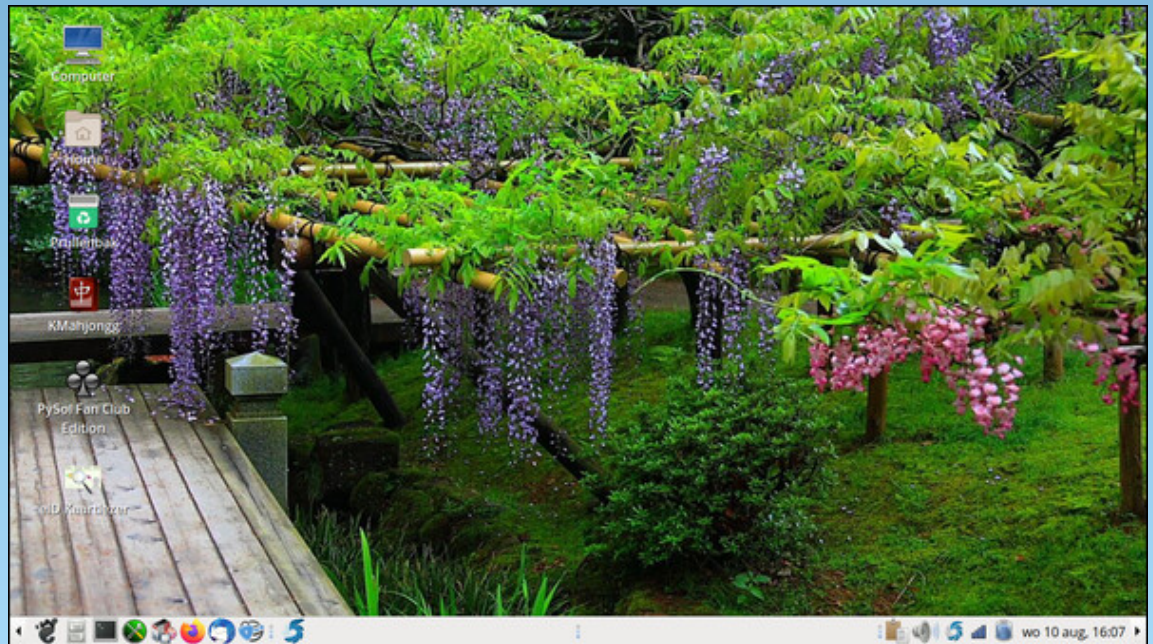
**PCLOS-Talk**  
Instant Messaging Server

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

Instant Messages

The advertisement features a cluster of colorful speech bubbles on the left and a single orange speech bubble on the right. The text is centered and uses a mix of blue and black fonts.

## Screenshot Showcase



Posted by mutse, on August 10, 2022, running Mate.

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!

# GIMP Tutorial: Make A Shadow Using Your Subject

by Meemaw

I saw [this](#) tutorial for creating a shadow, and thought it might be useful. Sometimes we want to create a different scene, but have some item we want to include. This may help.

I saw a car in a parade that I thought might look good in a different scene, so I'll put it in. You can do this too.

Open the background you want to use, and the car. The trick with mine was to cut the car out of the parade, and make sure everything was gone except the car. I didn't do the greatest job.... but it will work. I'm sure you will do an awesome job.



Copy & paste your subject into your background. Make sure your subject is on a transparent layer and not part of the background. You can paste it into your drawing but you have to choose for it to be a layer. Right click on the floating selection in the layers dialog and choose **New layer**. You can see the layer boundaries at center top.

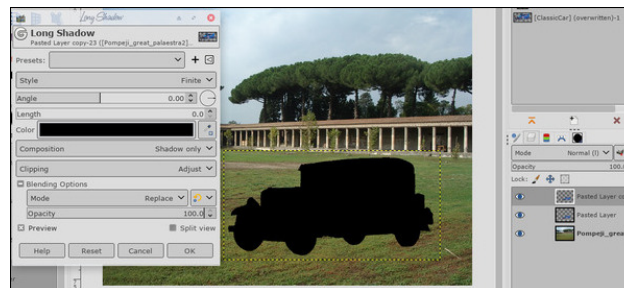
Next, duplicate your subject. Easy as choosing the layer and duplicating the layer. Then, go to **Filters > Light & Shadow > Long Shadow**.



Change the settings to the following:

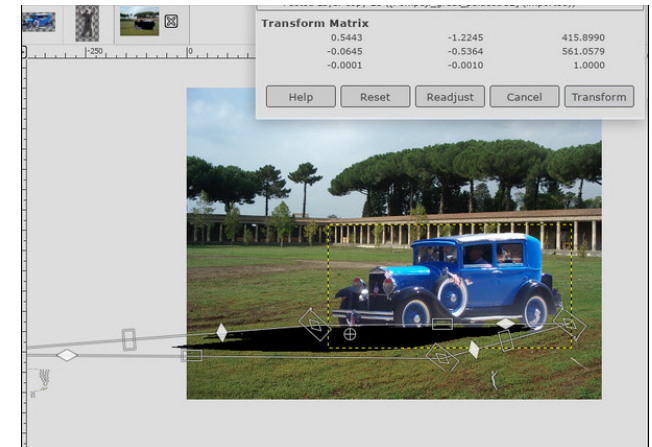
- Angle & Length both 0
- Shadow color - black
- Composition - Shadow only

Click OK.



We'll use **Unified Transform** - we learned about it in July. Click in the shadow and use the handles to move & place your shadow. Make sure you take into account the light source of your subject. Since the

light source is at the right in my picture, the shadow will be on the left. When you have it the way you want it, click **Transform**.



The good thing about this is that you can use the Transform tool again if it doesn't look as you want it. You can even use the paintbrush to add a bit to your shadow if you think it needs it.

Also, shadows are blurry, so use **Filters > Blur > Gaussian Blur** to blur the edges of the shadow. You could also use a gradient to fade out the shadow (depending on how you want it to look).

When you have it the way you want it, move the shadow layer underneath the subject layer so it looks more real (next page, top left)





Help PCLinuxOS Thrive & Survive

**DONATE**  
**TODAY**



Linux Docs  
Linux Man Pages



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.

## Screenshot Showcase



Posted by kalwisti, on August 2, 2022, running KDE.



# Nonprofit Websites Are Full Of Trackers. That Should Change.

by [Jason Kelley](#)

[Electronic Frontier Foundation](#)

Reprinted under Creative Commons Attribution license

*Jump straight to the [Online Privacy for Nonprofits Guide to Better Practices](#)*

Today, the vast majority of websites and emails that you encounter contain some form of tracking. Third-party cookies let advertisers follow you around the web; tracking pixels in emails confirm whether you've opened them; tracking links ensure websites know what you click; some websites even collect data on forms you've never actually submitted; still others share detailed interactions, such as appointments you've booked, with companies like Facebook. Each of these types of technology works by turning your actions into data: websites with tracking collect and store data about the site you are on, when, and what you are doing there; emails with tracking collect and store data about which email you opened and how you interacted with it.

All of this amounts to an incredible amount of data about you being collected without your permission. That data doesn't all end up in one place—sometimes it's collected by individual websites, sometimes by ad tech companies, and sometimes by third parties you've never heard of. But regardless of who has the data, it amounts to a massive violation of user privacy that can have far-reaching consequences. **Choosing to collect the data of supporters, clients and visitors isn't just a marketing, monetary or ideological decision: it's a decision that puts people in danger.** In a post-Roe world, for example, law enforcement might use internet search histories, online purchases, tracked locations, and other parts of a person's



digital trail [as evidence](#) of criminal intent – indeed, they already have.

If you are a nonprofit organization, you may be part of the problem. Unfortunately, a [2021 report from The Markup](#) showed that many nonprofits don't take threats to privacy seriously. That may be changing: Planned Parenthood, for example, [has suspended](#) the use of marketing trackers on some portions of their website in response to the dangers they could create for people seeking information on abortions. Hey Jane, an online provider of abortion pills, has [also removed](#) the Meta (Facebook) tracking pixel.

But there is still significantly more to do.

For example, you may use tools and software to improve the effectiveness of your marketing, and

they may in turn collect copious amounts of data on visitors and clients. That data is often shared with third parties, and from there could make its way to law enforcement or into court. And even if you are working in a space where data collection doesn't obviously endanger your clients or supporters, don't forget that what is currently legal may not always be legal. For example, in 2021 [legislatures in 22 states introduced bills](#) to ban or otherwise criminalize best practice medical care for transgender young people. There are also many laws that are vague or conflicting: many states have legalized cannabis, for example, but the federal government still considers it illegal.

Given all this, it's no stretch to say that the data you're collecting in order to further your mission could be weaponized against the very people you're



# Nonprofit Websites Are Full Of Trackers. That Should Change.

trying to support. Thankfully, it doesn't have to be that way, and we can prove it—and show you how to fight back.

**We've made a guide intended for any nonprofit or civil society group that cares about privacy. Not all of the advice may apply to you, but all of the principles should be helpful for thinking about steps to move you towards better privacy practices.**

We recognize that some nonprofits may rely on various forms of data collection, or even on the surveillance advertising ecosystem, and may be nervous about changing that. In the reproductive rights space, for example, Google Adwords or Facebook ads may be a critical way to drive users to accurate information. For other organizations, knowing how users arrived at a website can be essential to determining the cost-effectiveness of promotional choices.

It's reasonable to want to know whether an ad worked—but that knowledge comes at the price of handing information about your users and clients to the control of a third party.

Still, we understand many nonprofits may be reluctant to throw out all tracking or data collection, or the analytics tools that offer your organization important data. **We aren't asking you to do that.** Instead, our goal is to give you the knowledge necessary to consider what data collection and tracking is essential to your mission and what isn't, and to help you thrive while protecting the privacy of your supporters, clients, and users by finding alternative ways to get that information while respecting user privacy.

## What's Wrong With Tracking Your Users

Nonetheless, many ad tech companies argue that pervasive online tracking helps users by connecting them with services and products they want. But this

argument assumes that they want to be tracked by default. It ignores the damage done by the online surveillance ecosystem, particularly by [behavioral advertising](#). And it ignores the many [inaccurate or wrong](#) conclusions ad tech companies make. In fact, there's [plenty of evidence](#) that ad tech doesn't work nearly as well as it claims, in part due to the fraud that runs rampant in the industry. (EDRI's report, "Targeted Online" has a [detailed breakdown of problems](#) with the ad-tech industry if you'd like more information.)

**The reasons for NOT tracking are myriad:** First, you'll engender goodwill with your supporters. Second, you may not imagine your organization to be the likely target of ransomware or of a data breach, but the less data you collect, and the less you share with outside organizations or companies, the less likely that your supporters will be affected. Third, data privacy laws vary across regions, and we are in a time of rapid change with respect to those laws. Minimizing data collection and retention can help ensure you're complying with those laws.

Lastly, sensitive data on those in a variety of advocacy spaces has the potential to be weaponized by law enforcement. Whether you are a small or a large organization, holding onto significantly less data can make the legal process of discovery much less troubling for you—and for your supporters and clients.

It bears repeating: what is currently legal may not always be legal; administrations change, and what is criminalized (and what laws are enforced, and how) shifts. For example: there are currently a record number of bills that specifically target LGBTQ+ youth that have been introduced or passed in the past year, most of which criminalize speech and healthcare. If law enforcement are interested in who is seeking that healthcare information, nonprofits working in that space may be targeted, and the data they have—in house, on servers, or in the cloud—may all be relevant. And in a post-Roe world, organizations or website operators that work in the

reproductive rights space may receive subpoenas and warrants seeking user data that [could be employed](#) to prosecute abortion seekers, providers, and helpers. If Target can use recent purchases to [determine a person is likely pregnant](#), law enforcement can use the data trail a pregnant person creates online to determine that they are considering (or did consider) abortion—and they already have. And many of the privacy concerns that worry us today are just the latest example of issues that have already been happening to many other people.

Looking at all these reasons together, protecting privacy should be an obvious choice for most nonprofits and civil society organizations. And as if all this isn't enough, there are plenty of other ways to gain powerful insights about users and supporters without collecting individualized data about their online activity.

We know, because we walk the talk. For more than thirty years, EFF has fought to protect the rights of the user—the person who's making use of a technology, such as a website or a smartphone. For us, that includes giving users the ability to choose to not be tracked, to remain anonymous or private, and to not have their data collected without their permission. In keeping with that mission, here's what we do:

## This Website Does Not Track

On the surface, EFF's website looks pretty similar to other websites out there. But there's one major difference: we are preserving your privacy to the very best of our ability. Where most sites collect and store significant amounts of visitor data, like your IP address, location, browser, device type, and more, we log only a single byte of your IP address, as well as the referrer page (how you got here, if it's known), time stamp, user agent, language header, and a hash of all of this information. After seven days we keep only aggregate information from these logs.



## Nonprofit Websites Are Full Of Trackers. That Should Change.

We also geolocate IP addresses before anonymizing them and store only the country.

*Magazine Editor's note: The PCLinuxOS Magazine website uses NO trackers, whatsoever.*

(You can read more about our website's privacy practices [in our privacy policy](#).)

This means that we have less information on visitors than most websites—if we look back at who visited the site a week ago, we can see how many visits from which countries each page received, but not where they came from, for example. But that is good enough for us to make decisions for our site and our advocacy. And we think it's enough for most other nonprofits as well.

“But doesn't this make your work harder?” some of you may be asking. “How can you do research or marketing without these insights?” At times, yes, this lack of information makes our work very *slightly* more difficult. We rely on donors like you to support our work, and as an advocacy organization, we rely on digital activism to get the word out. Knowing which of our emails are the most read, or having easier access to detailed analytics data about the visitors to our website, could help us do both of these things slightly more effectively. But that would require us to collect large amounts of data about our users, supporters, and followers, and we don't believe the trade-off is worth it. (We also recognize that unlike many organizations, EFF has on-staff engineers to help determine privacy options and implement them. Still, most groups should be able to take at least some of the steps listed here.)

EFF is an active, growing, and successful organization—as are plenty of other privacy-respecting nonprofits, like the [Internet Archive](#) and [The Markup](#), not to mention companies like [Basecamp](#).

**So here's our challenge to other nonprofit organizations and civil society groups, and**

**companies, who care about user privacy: turn off tracking.**

**If you'd like to join us, you can visit: [Online Privacy for Nonprofits: A Guide to Better Practices](#).**



## Screenshot Showcase



Posted by francesco\_bat, on August 1, 2022, running Fluxbox.



# PCLinuxOS Recipe Corner Bonus



## American Goulash

Serves 6

### INGREDIENTS:

1 lb lean (at least 80%) ground beef  
1 medium yellow onion, chopped  
2 cloves garlic, finely chopped  
1 1/2 cups (from 32-oz carton) beef flavored broth  
1 can (15 oz) tomato sauce  
1 can (14.5 oz) fire roasted diced tomatoes, undrained  
1 tablespoon Italian seasoning  
1 teaspoon paprika  
1/4 teaspoon black pepper  
1 cup uncooked elbow macaroni  
3 oz cream cheese, cubed  
1 cup shredded Monterey Jack cheese (4 oz)  
1/2 cup flavored croutons, coarsely crushed

### DIRECTIONS:

Heat in a 12-inch nonstick skillet over medium-high heat; add beef and onion. Cook 7 to 9 minutes, stirring frequently, until beef is brown; drain, and return to skillet. Add garlic; cook for about 1 minute or until garlic is fragrant. Stir in broth, tomato sauce, tomatoes, Italian seasoning, paprika and pepper.

Heat to simmering, stirring occasionally. Reduce heat; cover and simmer for about 20 minutes or until slightly thickened.

Stir in macaroni; cover and cook for 16 to 18 minutes, stirring occasionally, until pasta is tender. Stir in cream cheese until completely melted, about 3 minutes. Sprinkle with shredded cheese; top with crushed croutons.



### TIPS:

If you don't have Italian seasoning, substitute 1 teaspoon each of dried basil, dried oregano and dried rosemary in the recipe.

Don't have macaroni? Substitute penne or rotini pasta.

### NUTRITION:

Calories: 410      Carbs: 33g      Fiber: 3g  
Sodium: 805mg      Protein: 24g



The  
PCLinuxOS  
Magazine

Created with  
Scribus

# PCLinuxOS Puzzled Partitions

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

**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.

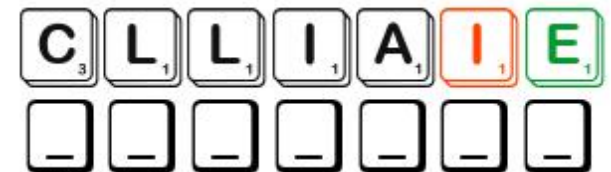
Each column must contain all of the numbers 1 through 9 and no two numbers in the same column of a Sudoku puzzle can be the same. Each row must contain all of the numbers 1 through 9 and no two numbers in the same row of a Sudoku puzzle can be the same.

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 231, average score 162.

Download Puzzle Solutions Here



# Word Find: September, 2022

## Flowers

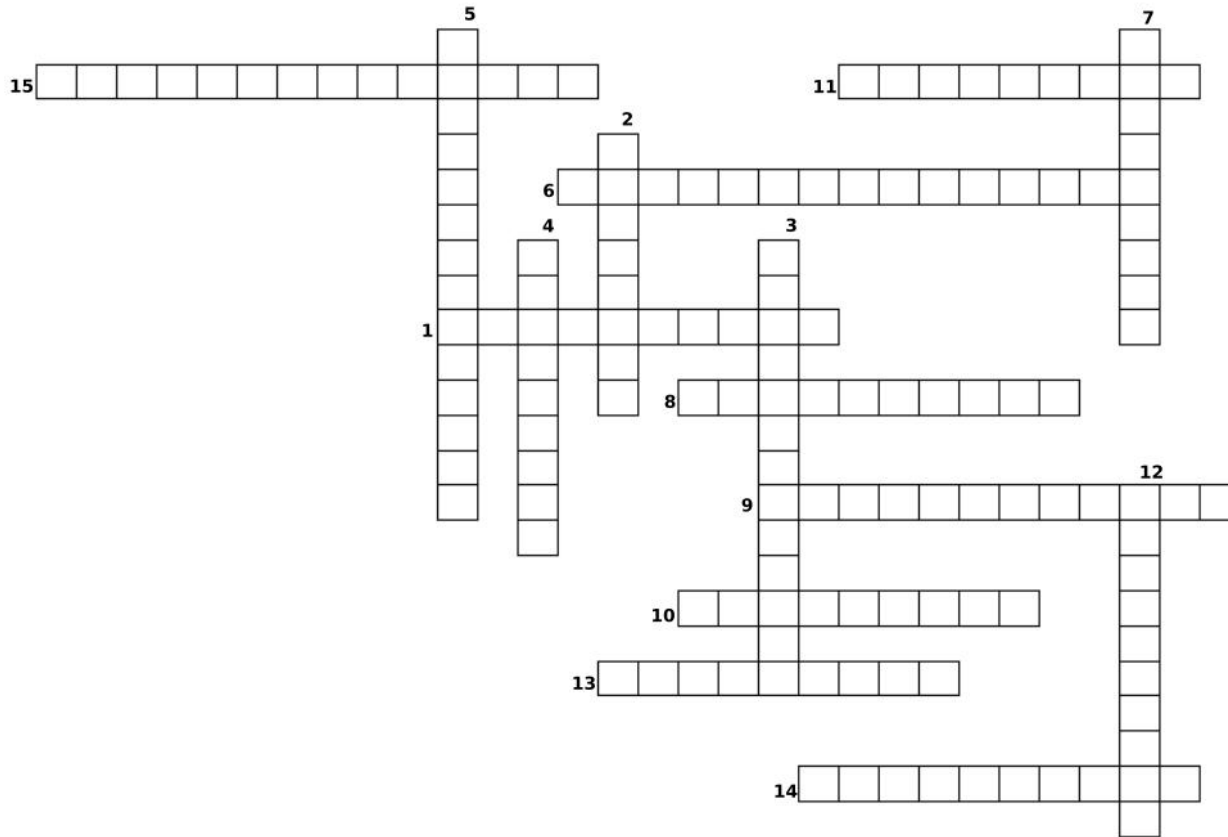
G U V V E N U S F L Y T R A P D E H D H P O Y A T O B E N V  
 G G E J E N Y S H L H W F H S S Z Y I I U N D E Y G W F N F  
 O Y H D R H O D O D E N D R O N I D V N T M F L O D U O A J  
 W N V N V Q A A E S P W S Y E L N R I Q E B I L D C M X S G  
 L R Y U C C A F L O W E R U S Z N A M H R L D I A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

- |                 |                    |
|-----------------|--------------------|
| ANEMONE         | APPLE BLOSSOM      |
| BEGONIA         | BELLFLOWER         |
| BLACKEYED SUSAN | BLUE BONNET        |
| BOUGAINVILLEA   | CALENDULA          |
| CALLA LILY      | CAMELLIA           |
| CHRYSANTHEMUM   | DELPHINIUM         |
| DIANTHUS        | EDELWEISS          |
| GILLYFLOWER     | GLADIOLUS          |
| GOLDENROD       | HAWTHORN           |
| HOLLYHOCK       | HONEYSUCKLE        |
| HYDRANGEA       | LILY OF THE VALLEY |
| MAGNOLIA        | MAYFLOWER          |
| MORNING GLORY   | NARCISSUS          |
| NASTURTIUM      | OLEANDER           |
| PASSION FLOWER  | QUEEN ANNE'S LACE  |
| RANUNCULUS      | RHODODENDRON       |
| SNAPDRAGON      | SUNFLOWER          |
| TIGER LILY      | VENUS FLYTRAP      |
| WOLFSBANE       | YUCCA FLOWER       |
| ZINNIA          |                    |

[Download Puzzle Solutions Here](#)



# Flowers Crossword



1. A perennial plant of the buttercup family, especially any of several tall cultivated varieties having palmate leaves and long racemes of showy, variously colored spurred flowers.
2. A genus of about 340 species of flowering plants. Common names include carnation, pink and sweet william.
3. Any of several woody shrubs or vines having small flowers surrounded by large usually bright red or purple bracts.
4. A Mediterranean annual plant in the composite family, widely cultivated for its showy, yellow or orange, rayed flower heads that were formerly used in medicine, coloring, and flavoring of food.
5. A North American coneflower having flower heads with deep yellow to orange rays and dark conical disks
6. A widely cultivated ornamental plant having one-sided racemes of fragrant, bell-shaped white flowers.
7. A tall plant in the mallow family, native to the Middle East and widely cultivated for its showy clusters of very large, variously colored flowers.
8. Any of several plants of the figwort family, widely cultivated for its showy racemes of two-lipped, variously colored flowers.
9. A carnivorous plant native to subtropical wetlands on the East Coast of the United States. It catches & eats its prey—chiefly insects and arachnids.
10. A plant of the genus *Aconitum*; aconite or monk's-hood.
11. Any of numerous chiefly North American plants having clusters of small usually yellow flower heads that bloom in late summer or fall.
12. Any of numerous plants, having yellow or white usually five-petaled flowers, and including the buttercups and the crowfoots.
13. Any of various shrubs, having opposite leaves and large, flat-topped or rounded clusters of white, pink, or blue flowers.
14. Any of various plants, native to South and Central America, that have round leaves and pungent edible yellow, orange, or red spurred flowers and are often grown as ornamentals.
15. A widely naturalized Eurasian biennial herb which has a whitish acrid taproot and flat lacelike clusters of tiny white flowers and from which the cultivated carrot originated.

[Download Puzzle Solutions Here](#)

# Mixed-Up-Meme Scrambler



What she hoped to meet  
on the singles cruise.

A " \_\_\_\_\_ "

BAIDE

—   —

LYMAN

— —

NATTYR

— —

PULCEO

—  — —  —

[Download Puzzle Solutions Here](#)

# More Screenshot Showcase



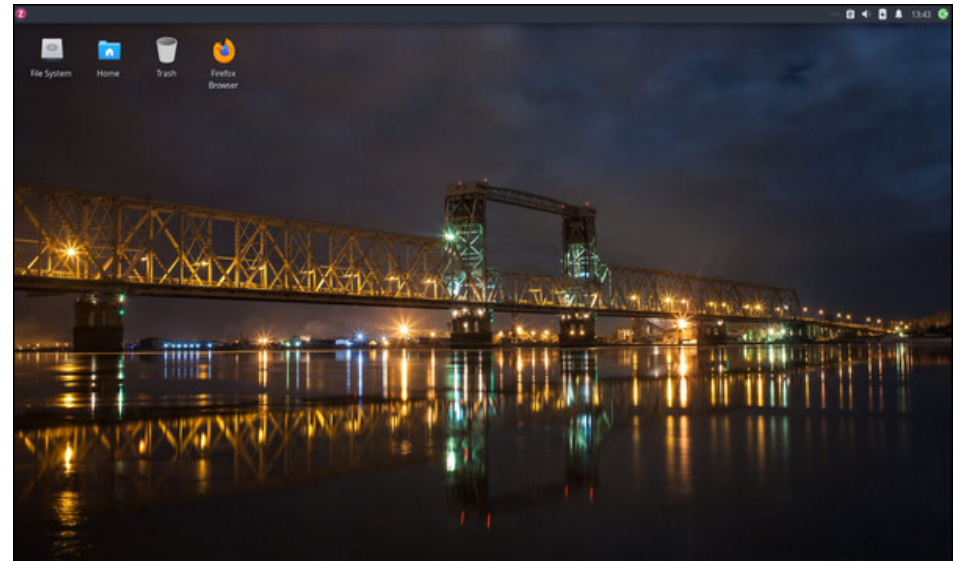
Posted by dxgiusti, on August 5, 2022, running KDE.



Posted by DrMop, on August 23, 2022, running Xfce.



Posted by brisvegas, on August 1, 2022, running Mate.



Posted by ar4ox, on August 10, 2022, running KDE.