The PCLinuxOS magazine

Volume 175

August, 2021

In This Issue...

The PCLinuxOS magazine

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

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

Visit us online at 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
Pete Kelly
Alessandro Ebersol
Cg_Boy
YouCanToo
Daniel Meiß-Wilhelm

Contributors:
Ramchu
The Cat

From The Chief Editor's Desk...

One of the things that stands out about PCLinuxOS is the sense of community that PCLinuxOS forum visitors find among its users. Time and time again, I see it mentioned in the forum.

Even though we all come from different backgrounds, walks of life, professions, and have varied interests, one thing ties us all together: our love of Texstar's creation, PCLinuxOS. In many ways, those friends we make in the forum become lifelong friends, and perhaps even extended family members.

Many of us will never meet in person. But, through our interactions with one another on the forum, we become close. We become friends. We share our successes and failures. We squabble with one another. We laugh with one another. We feel for one another.

That sounds like a family to me.

Like in all families, there are the occasional clowns. There are the occasional rabble rousers. There are dysfunctional members. There are calming members. But at the end of the day, we are all still family.

Some members of that family may move away, to graze in other pastures. Some may even drop back by to check in and say howdy from time to time. But many will move on with nary a peep or utterance to be heard ever again.

That leaves many of us that are left behind to wonder *"whatever happened to __________"* (fill in the blank). With some, like Sproggy, Tara Rains, and Joble, they are taken from us before their time, and will never be heard from again. But, with most, they are still wandering around Linux-land.

Wouldn't it be nice if they dropped in from time to time to let us know what they have been up to? Those family ties remain, even after a user leaves PCLinuxOS for other pastures. Friendships and relationships were built during their stay, and remain long after their departure.

One such user, Dadster, did exactly that. He had moved on to Mint Linux, but stopped by the PCLinuxOS forum to see how we all were doing. He admitted that he maintains a soft spot in his heart for PCLinuxOS, and the community that has grown up around it. Even though it had been a while since being seen around the PCLinuxOS forum, he was remembered and welcomed back.

It would be nice if more former PCLinuxOS users did the same. If nothing else, it gives the rest of us an idea of what the former user has been up to, and lets us know that we have not been forgotten amidst the former user's new adventures.

Until next month, I bid you peace, happiness, serenity, prosperity, and good health. Be careful out there with the newest surge of the COVID19 delta variant! This is some NASTY stuff!

Happy 30th Birthday, Linux!

by Paul Arnote (parnote)

Thirty years ago, on August 25, the computing landscape changed. Forever. The date is easy for me to remember. Linux and I share the same birthday (albeit a few decades apart).

Enrolled in the University of Helsinki, a young Linus Torvalds had gotten his hands on a 386 computer – state of the art in its day. It was Intel's first 32 bit processor, and he wanted to be able to unlock its potential. There was a Unix operating system available for free, but only for educational purposes. It was called Minix. Its creator would not allow its source code to be altered, and largely ignored user requests for features. Minix featured, among other things, a modular kernel, in the belief that it would be easier to maintain. Unfortunately, it was only a 16 bit design, and its creator was reluctant to make a 32 bit version. All other Unix systems available for the new 32 bit platform were prohibitively expensive for regular, individual users.

Thus, Linus Torvalds set out to make his own free kernel. At first, he built Linux on a computer running Minix, but ensured that Linux was free of proprietary Minix code. The rest of the story has been told and retold over the years, and is easily found on the internet.

So, for Linux's birthday, I want to rerun the brunt of an article we ran in 2016. About a year after releasing Linux to the public, Linus Torvalds gathered up many of the Usenet posts and correspondence from the time around Linux's release. What follows is Linus Torvald's account of Linux History, in the form of the communications that took place at the time.

LINUX's History

Note: The following text was written by Linus on July 31 1992. It is a collection of various artifacts from the period in which Linux first began to take shape.

This is just a sentimental journey into some of the first posts concerning linux, so you can happily press 'n' now if you actually thought you'd get anything technical.

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: Gcc-1.40 and a posix-question
Message-ID:
Date: 3 Jul 91 10:00:50 GMT

Hello netlanders,

Due to a project I'm working on (in minix), I'm interested in the posix standard definition. Could somebody please point me to a (preferably) machine-readable format of the latest posix rules? Ftp-sites would be nice.

The project was obviously linux, so by July 3rd I had started to think about actual user-level things: some of the device drivers were ready, and the harddisk actually worked. Not too much else.

As an aside for all using gcc on minix - [deleted]

Just a success-report on porting gcc-1.40 to minix using the 1.37 version made by Alan W Black & co.

Linus Torvalds torvalds@kruuna.helsinki.fi

PS. Could someone please try to finger me from overseas, as I've installed a "changing .plan" (made by your's truly), and I'm not certain it works from outside? It should report a new .plan every time.

So I was clueless - had just learned about named pipes. Sue me. This part of the post got a lot more response than the actual POSIX query, but the query did lure out arl from the woodwork, and we mailed around for a bit, resulting in the Linux subdirectory on nic.funet.fi.

Then, almost two months later, I actually had something working: I made sources for version 0.01 available on nic sometimes around this time. 0.01 sources weren't actually runnable: they were just a token gesture to arl who had probably started to despair about ever getting anything. This next post must have been from just a couple of weeks before that release.

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: What would you like to see most in minix?
Summary: small poll for my new operating system
Message-ID:
Date: 25 Aug 91 20:57:08 GMT
Organization: University of Helsinki

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready.I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want.Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torvalds@kruuna.helsinki.fi)

PS.Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT prowell table (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

Judging from the post, 0.01 wasn't actually out yet, but it's close. I'd guess the first version went out in the middle of September -91. I got some responses to this (most by mail, which I haven't saved), and I even got a few mails asking to be beta-testers for linux. After that
just a few general answers to questions on the net:

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: Re: What would you like to see most in minix?
Summary: yes - it's nonportable
Message-ID:
Date: 26 Aug 91 11:06:02 GMT
Organization: University of Helsinki

In articit is hard no matter what way you look at it
lejkp@cs.HUT.FI (Jyrki Kuoppala) writes:
>> [re: my post about my new OS]
>
>Tell us more!Does it need a MMU?

Yes, it needs a MMU (sorry everybody), and it specifically needs a 386/486 MMU (see later).

>
>>PS.Yes - it's free of any minix code, and it has a multi-threaded fs.
>>It is NOT protable (uses 386 task switching etc)
>
>How much of it is in C?What difficulties will there be in porting?
>Nobody will believe you about non-portability ;-), and I for one would
>like to port it to my Amiga (Mach needs a MMU and Minix is not free).

Simply, I'd say that porting is impossible. It's mostly in C, but most people wouldn't call what I write C. It uses every conceivable feature of the 386 I could find, as it was also a project to teach me about the 386. As already mentioned, it uses a MMU, for both paging (not to disk
yet) and segmentation. It's the segmentation that makes it REALLY 386 dependent (every task has a 64Mb segment for code & data - max 64 tasks in 4Gb. Anybody who needs more than 64Mb/task - tough cookies).

It also uses every feature of gcc I could find, specifically the __asm__ directive, so that I wouldn't need so much assembly language objects. Some of my "C"-files (specifically mm.c) are almost as much assembler as C. It would be "interesting" even to port it to another compiler (though why anybody would want to use anything other than gcc is a mystery).

Note: linux has in fact gotten more portable with newer versions: there was a lot more assembly in the early versions. It has in fact been ported to other architectures by now.

Unlike minix, I also happen to LIKE interrupts, so interrupts are handled without trying to hide the reason behind them (I especially like my hard-disk-driver.Anybody else make interrupts drive a state-machine?).All in all it's a porters nightmare.

>As for the features; well, pseudo ttys, BSD sockets, user-mode
>filesystems (so I can say cat /dev/tcp/kruuna.helsinki.fi/finger),
>window size in the tty structure, system calls capable of supporting
>POSIX.1.Oh, and bsd-style long file names.

Most of these seem possible (the tty structure already has stubs for window size), except maybe for the user-mode filesystems. As to POSIX, I'd be delighted to have it, but posix wants money for their papers, so that's not currently an option. In any case these are things that won't be supported for some time yet (first I'll make it a simple minix-lookalike, keyword SIMPLE).

Linus (torvalds@kruuna.helsinki.fi)

PS. To make things really clear - yes I can run gcc on it, and bash, and most of the gnu [bin/file]utilities, but it's not very debugged, and the library is really minimal. It doesn't even support floppy-disks yet. It won't be ready for distribution for a couple of months. Even then it probably won't be able to do much more than minix, and much less in some respects. It will be free though (probably under gnu-license or similar).

Well, obviously something worked on my machine: I doubt I had yet gotten gcc to compile itself under linux (or I would have been too proud of it not to mention it). Still before any release-date.

Then, October 5th, I seem to have released 0.02. As I already mentioned, 0.01 didn't actually come with any binaries: it was just source code for people interested in what linux looked like. Note the lack of announcement for 0.01: I wasn't too proud of it, so I think I only sent a note to everybody who had shown interest.

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: Free minix-like kernel sources for 386-AT
Message-ID:
Date: 5 Oct 91 05:41:06 GMT
Organization: University of Helsinki

Do you pine for the nice days of minix-1.1, when men were men and wrote their own device drivers? Are you without a nice project and just dying to cut your teeth on a OS you can try to modify for your needs? Are you finding it frustrating when everything works on minix? No more all-nighters to get a nifty program working? Then this post might be just for you :-)

As I mentioned a month(?) ago, I'm working on a free version of a minix-lookalike for AT-386 computers. It has finally reached the stage where it's even usable (though may not be depending on what you want), and I am willing to put out the sources for wider distribution. It is just version 0.02 (+1 (very small) patch already), but I've successfully run bash/gcc/gnu-make/gnu-sed/compress etc under it.

Sources for this pet project of mine can be found at nic.funet.fi (128.214.6.100) in the directory /pub/OS/Linux.The directory also contains some README-file and a couple of binaries to work under linux (bash, update and gcc, what more can you ask for :-). Full kernel source is provided, as no minix code has been used.Library sources are only partially free, so that cannot be distributed currently. The system is able to compile "as-is" and has been known to work.Heh. Sources to the binaries (bash and gcc) can be found at the same place in /pub/gnu.

ALERT! WARNING! NOTE! These sources still need minix-386 to be compiled (and gcc-1.40, possibly 1.37.1, haven't tested), and you need minix to set it up if you want to run it, so it is not yet a standalone system for those of you without minix. I'm working on it. You also need to be something of a hacker to set it up (?), so for those hoping for an alternative to minix-386, please ignore me. It is currently meant for hackers interested in operating systems and 386's with access to minix.

The system needs an AT-compatible harddisk (IDE is fine) and EGA/VGA. If you are still interested, please ftp the README/RELNOTES, and/or mail me for additional info.

I can (well, almost) hear you asking yourselves "why?". Hurd will be out in a year (or two, or next month, who knows), and I've already got minix. This is a program for hackers by a hacker.I've enjouyed doing it, and somebody might enjoy looking at it and even modifying it for their own needs.It is still small enough to understand, use and modify, and I'm looking forward to any comments you might have.

I'm also interested in hearing from anybody who has written any of the utilities/library functions for minix. If your efforts are freely distributable (under copyright or even public domain), I'd like to hear from you, so I can add them to the system. I'm using Earl Chews estdio right now (thanks for a nice and working system Earl), and similar works will be very wellcome. Your (C)'s will of course be left intact. Drop me a line if you are willing to let me use your code.

Linus

PS. to PHIL NELSON! I'm unable to get through to you, and keep getting "forward error - strawberry unknown domain" or something.

TUX TURNS 30!
This could be "the year of the Linux desktop." Happy Birthday.
#TuxTurns30
THE LINUX FOUNDATION

Well, it doesn't sound like much of a system, does it? It did work, and some people even tried it out. There were several bad bugs (and there was no floppy-driver, no VM, no nothing), and 0.02 wasn't really very usable.

0.03 got released shortly thereafter (max 2-3 weeks was the time between releases even back then), and 0.03 was pretty usable. The next version was numbered 0.10, as things actually started to work pretty well. The next post gives some idea of what had happened in two more months...

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: Re: Status of LINUX?
Summary: Still in beta
Message-ID:
Date: 19 Dec 91 23:35:45 GMT
Organization: University of Helsinki

In articlemiquels@maestro.htsa.aha.nl (Miquel van Smoorenburg) writes:

>Hello *,
>I know some people are working on a FREE O/S for the 386/486,
>under the name Linux. I checked nic.funet.fi now and then, to see what was
>happening. However, for the time being I am without FTP access so I don't
>know what is going on at the moment. Could someone please inform me about it?
>It's maybe best to follow up to this article, as I think that there are
>a lot of potential interested people reading this group. Note, that I don't
>really *have* a >= 386, but I'm sure in time I will.

Linux is still in beta (although available for brave souls by ftp), and has reached the version 0.11.It's still not as comprehensive as 386-minix, but better in some respects.The "Linux info-sheet" should be posted here some day by the person that keeps that up to date.In the meantime, I'll give some small pointers.

First the bad news:

- Still no SCSI: people are working on that, but no date yet. Thus you need a AT-interface disk (I have one report that it works on an EISA 486 with a SCSI disk that emulates the AT-interface, but that's more of a fluke than anything else: ISA+AT-disk is currently the hardware setup)

As you can see, 0.11 had already a small following. It wasn't much, but it did work.

- still no init/login: you get into bash as root upon bootup.

That was still standard in the next release.

- although I have a somewhat working VM (paging to disk), it's not ready yet. Thus linux needs at least 4M to be able to run the GNU binaries (especially gcc).It boots up in 2M, but you cannot compile.

I actually released a 0.11+VM version just before Christmas -91: I didn't need it myself, but people were trying to compile the kernel in 2MB and failing, so I had to implement it. The 0.11+VM version was available only to a small number of people that wanted to test it out: I'm still surprised it worked as well as it did.

- minix still has a lot more users: better support.

- it hasn't got years of testing by thousands of people, so there are probably quite a few bugs yet.

Then for the good things..

- It's free (copyright by me, but freely distributable under a very lenient copyright)

The early copyright was in fact much more restrictive than the GNU copyleft: I didn't allow any money at all to change hands due to linux. That changed with 0.12.

- it's fun to hack on.

- /real/ multithreading filesystem.

- uses the 386-features.Thus locked into the 386/486 family, but it makes things clearer when you don't have to cater to other chips.

- a lot more... read my .plan.

/I/ think it's better than minix, but I'm a bit prejudiced.It will never be the kind of professional OS that Hurd will be (in the next century or so :), but it's a nice learning tool (even more so than minix, IMHO), and it was/is fun working on it.

Linus (torvalds@kruuna.helsinki.fi)

---- my .plan --------------------------
Free UNIX for the 386 - coming 4QR 91 or 1QR 92.

The current version of linux is 0.11 - it has most things a unix kernel needs, and will probably be released as 1.0 as soon as it gets a little more testing, and we can get a init/login going. Currently you get dumped into a shell as root upon bootup.

Linux can be gotten by anonymous ftp from 'nic.funet.fi' (128.214.6.100) in the directory '/pub/OS/Linux'.The same directory also contains some binary files to run under Linux.Currently gcc, bash, update, uemacs, tar, make and fileutils.Several people have gotten a running system, but it's still a hackers kernel.

Linux still requires a AT-compatible disk to be useful: people are working on a SCSI-driver, but I don't know when it will be ready.

There are now a couple of other sites containing linux, as people have had difficulties with connecting to nic. The sites are:

Tupac-Amaru.Informatik.RWTH-Aachen.DE (137.226.112.31):
directory /pub/msdos/replace

tsx-11.mit.edu (18.172.1.2):
directory /pub/linux

There is also a mailing list set up 'Linux-activists@niksula.hut.fi'. To join, mail a request to 'Linux-activists-request@niksula.hut.fi'. It's no use mailing me: I have no actual contact with the mailing-list (other than being on it, naturally).

Mail me for more info:

Linus (torvalds@kruuna.Helsinki.FI)

0.11 has these new things:

- **demand loading**
- **code/data sharing between unrelated processes**
- **much better floppy drivers (they actually work mostly)**

- bug-corrections
- support for Hercules/MDA/CGA/EGA/VGA
- the console also beeps (WoW! Wonder-kernel :-)
- mkfs/fsck/fdisk
- US/German/French/Finnish keyboards
- settable line-speeds for com1/2

As you can see: 0.11 was actually stand-alone: I wrote the first mkfs/fsck/fdisk programs for it, so that you didn't need minix any more to set it up. Also, serial lines had been hard-coded to 2400bps, as that was all I had.

Still lacking:
- init/login
- rename system call
- named pipes
- symbolic links

Well, they are all there now: init/login didn't quite make it to 0.12, and rename() was implemented as a patch somewhere between 0.12 and 0.95. Symlinks were in 0.95, but named pipes didn't make it until 0.96.

Note: The version number went directly from 0.12 to 0.95, as the follow-on to 0.12 was getting feature-full enough to deserve a number in the 0.90's

0.12 will probably be out in January (15th or so), and will have:
- POSIX job control (by tytso)
- VM (paging to disk)
- Minor corrections

Actually, 0.12 was out January 5th, and contained major corrections. It was in fact a very stable kernel: it worked on a lot of new hardware, and there was no need for patches for a long time. 0.12 was also the kernel that "made it": that's when Linux started to spread a lot faster. Earlier kernel releases were very much only for hackers: 0.12 actually worked quite well.

30TH
ANNIVERSARY
OF LINUX
1991-2021
#30YearsofLinux
100% of the world's top 500 supercomputers run on Linux. Not bad for 30.
THE LINUX FOUNDATION

Note: The following document is a reply by Linus Torvalds, creator of Linux, in which he talks about his experiences in the early stages of Linux development

To: Linux-Activists@BLOOM-PICAYUNE.MIT.EDU
From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Subject: Re: Writing an OS - questions !!
Date: 5 May 92 07:58:17 GMT

In articlenani@td2cad.intel.com (V. Narayanan) writes:

Hi folks,

For quite some time this "novice" has been wondering as to how one goes about the task of writing an OS from "scratch". So here are some questions, and I would appreciate if you could take time to answer 'em.

Well, I see someone else already answered, but I thought I'd take on the linux-specific parts.Just my personal experiences, and I don't know how normal those are.

1) How would you typically debug the kernel during the development phase?

Depends on both the machine and how far you have gotten on the kernel: on more simple systems it's generally easier to set up. Here's what I had to do on a 386 in protected mode.

The worst part is starting off: after you have even a minimal system you can use printf etc, but moving to protected mode on a 386 isn't fun, especially if you at first don't know the architecture very well. It's distressingly easy to reboot the system at this stage: if the 386 notices something is wrong, it shuts down and reboots - you don't even get a chance to see what's wrong.

Printf() isn't very useful - a reboot also clears the screen, and anyway, you have to have access to video-mem, which might fail if your segments are incorrect etc. Don't even think about debuggers: no debugger I know of can follow a 386 into protected mode. A 386 emulator might do the job, or some heavy hardware, but that isn't usually feasible.

What I used was a simple killing-loop: I put in statements like

```
die: jmp die
```

at strategic places. If it locked up, you were ok, if it rebooted, you knew at least it happened before the die-loop. Alternatively, you might use the sound io ports for some sound-clues, but as I had no experience with PC hardware, I didn't even use that. I'm not saying this is the only way: I didn't start off to write a kernel, I just wanted to explore the 386 task-switching primitives etc, and that's how I started off (in about April-91).

After you have a minimal system up and can use the screen for output, it gets a bit easier, but that's when you have to enable interrupts. Bang, instant reboot, and back to the old way. All in all, it took about 2 months for me to get all the 386 things pretty well sorted out so that I no longer had to count on avoiding rebooting at once, and having the basic things set up (paging, timer-interrupt and a simple task-switcher to test out the segments etc).

2) Can you test the kernel functionality by running it as a process on a different OS? Wouldn't the OS(the development environment) generate exceptions in cases when the kernel (of the new OS) tries to modify 'priviledged' registers?

Yes, it's generally possible for some things, but eg device drivers usually have to be tested out on the bare machine. I used minix to develop linux, so I had no access to IO registers, interrupts etc. Under DOS it would have been possible to get access to all these, but then you don't have 32-bit mode. Intel isn't that great - it would probably have been much easier on a 68040 or similar.

So after getting a simple task-switcher (it switched between two processes that printed AAAA...and BBBB...respectively by using the timer-interrupt - Gods I was proud over that), I still had to continue debugging basically by using printf. The first thing written was the keyboard driver: that's the reason it's still written completely in assembler (I didn't dare move to C yet - I was still debugging at about instruction-level).

After that I wrote the serial drivers, and voila, I had a simple terminal program running (well, not that simple actually). It was still the same two processes (AAA..), but now they read and wrote to the console/serial lines instead. I had to reboot to get out of it all, but it was a simple kernel.

After that is was plain sailing: hairy coding still, but I had some devices, and debugging was easier. I started using C at this stage, and it certainly speeds up developement. This is also when I start to get serious about my megalomaniac ideas to make "a better minix that minix". I was hoping I'd be able to recompile gcc under linux some day...

The harddisk driver was more of the same: this time the problems with bad documentation started to crop up. The PC may be the most used architecture in the world right now, but that doesn't mean the docs are any better: in fact I haven't seen /any/ book even mentioning the weird 386-387 coupling in an AT etc (Thanks Bruce).

After that, a small filesystem, and voila, you have a minimal unix. Two months for basic setups, but then only slightly longer until I had a disk-driver (seriously buggy, but it happened to work on my machine) and a small filesystem. That was about when I made 0.01 available (late august-91? Something like that): it wasn't pretty, it had no floppy driver, and it couldn't do much anything.I don't think anybody ever compiled that version. But by then I was hooked, and didn't want to stop until I could chuck out minix.

3) Would new linkers and loaders have to be written before you get a basic kernel running?

All versions up to about 0.11 were cross-compiled under minix386 - as were the user programs. I got bash and gcc eventually working under 0.02, and while a race-condition in the buffer-cache code prevented me from recompiling gcc with itself, I was able to tackle smaller compiles. 0.03 (October?) was able to recompile gcc under itself, and I think that's the first version that anybody else actually used. Still no floppies, but most of the basic things worked.

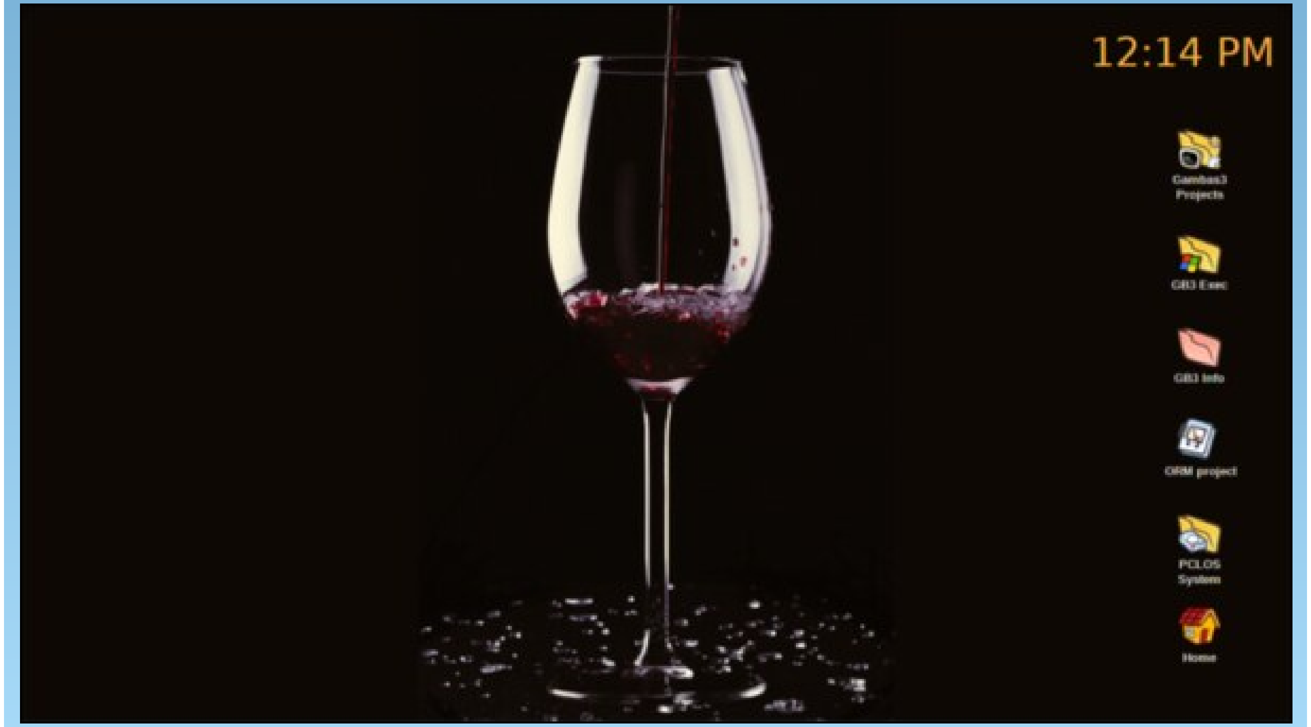
After 0.03 I decided that the next version was actually useable (it was, kind of, but boy is X under 0.96 more impressive), and I called the next version 0.10 (November?). It still had a rather serious bug in the buffer-cache handling code, but after patching that, it was pretty ok. 0.11 (December) had the first floppy driver, and was the point where I started doing linux developement under itself. Quite as well, as I trashed my minix386 partition by mistake when trying to autodial /dev/hd2.

By that time others were actually using linux, and running out of memory. Especially sad was the fact that gcc wouldn't work on a 2MB machine, and although c386 was ported, it didn't do everything gcc did, and couldn't recompile the kernel. So I had to implement disk-paging: 0.12 came out in January (?) and had paging by me as well as job control by tytso (and other patches: pmacdona had started on VC's etc). It was the first release that started to have "non-essential" features, and being partly written by others. It was also the first release that actually did many things better than minix, and by now people started to really get interested.

Then it was 0.95 in March, bugfixes in April, and soon 0.96. It's certainly been fun (and I trust will continue to be so) - reactions have been mostly very positive, and you do learn a lot doing this type of thing (on the other hand, your studies suffer in other respects :)

Linus

Screenshot Showcase



Posted by bb64, July 25, 2021, running Xfce.

PCLinuxOS Recipe Corner

Home-Style Beef & Potato Skillet

Servings 4
Unit converter

INGREDIENTS:

1 lb lean (at least 80%) ground beef (453.5 g)
4 medium green onions, chopped (1/4 cup) (26 g)
1 cup water (237 ml)
1/2 teaspoon garlic salt (1.5 g)
1 package (0.87 oz) onion gravy mix (28.3 g)
2 cups frozen potatoes O'Brien with onions
    and peppers (from 24-oz bag) (256 g)
1/2 cup frozen baby sweet peas (64 g)
1 large tomato, chopped (1 cup) (200 g)
1 1/2 cups Original Bisquick™ mix ** (192 g)
1/2 cup water (118 g)
** See our homemade Bisquick Mix here.

DIRECTIONS:

1. In a 10-inch skillet, cook beef over medium-high heat 5 to 7 minutes, stirring occasionally, until brown; drain. Stir in 2 tablespoons of the onions, 1 cup water, the garlic salt and gravy mix (dry). Cook, stirring constantly, until mixture thickens. Stir in potatoes, peas and tomato. Heat until hot; reduce heat to medium-low.

2. In a small bowl, stir the Bisquick mix, remaining 2 tablespoons of onions and 1/2 cup water until soft dough forms. Drop dough by tablespoonfuls (see tips) onto beef mixture.

3. Cover; cook for 8 minutes. Uncover; cook 8 to 10 minutes longer or until a toothpick inserted in the center of the dumplings comes out clean.

TiPS:

When making dumplings, a great way to drop the dough is to use a small cookie-dough scoop, quickly scooping dough and dropping onto the beef mixture.

NUTRITION:

Calories: 360	Carbs: 44g	Fiber: 5g
Sodium: 820mg	Protein: 27g	

PCLinuxOS Recipe Corner Extra

Homemade Strawberry Pie

by Ramchu

This is an easy to make Strawberry Pie recipe, that is delicious and requires no special ingredients.

You will need:

1 - 9 inch pie pan (22.9cm)
1 - 9 inch pie crust (store bought or make your own)
7 - cups strawberries (1.7L)
1 1/4- cup sugar (250g)
3 - Tbsp. corn starch (44g)
3/4 - cup cold water (177ml)
Whipped topping

Directions

Place the pie crust in the pie pan and bake at 400 F (204 C) for 20 minutes or until golden brown, remove from the oven and let cool.

Take 3 cups (711ml) of strawberries, place in a bowl and mash (I use an old style potato masher) add the sugar and stir, place mixture in a cooking pan/pot and cook over medium heat until sugar is dissolved.

Mix 3 Tbsp. (44g) corn starch with 3/4 cup (177ml) cold water, stir well to mix and slowly add to strawberry mixture stirring constantly until it thickens and becomes translucent.

Gently fold the remaining 4 cups (948ml) of strawberries into the thickened strawberry mixture until they are coated.

Pour the strawberry mixture into the pre-baked pie crust and refrigerate for several hours.

Serve topped with a large spoonful of whipped topping.

Inkscape Tutorial: New Release Highlights

by Meemaw

Inkscape 1.1 was released on May 24, 2021. It’s the latest major Inkscape release. Let’s look at some of the new features.

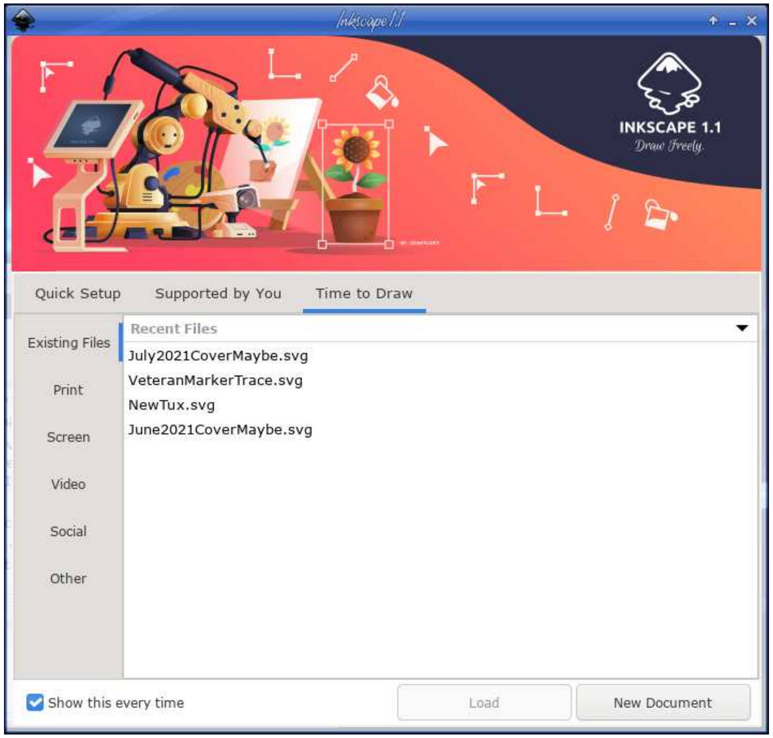
--- A **Welcome dialog**, which is different. Choices for a new document's size or file to open are available. In the left column under “Time to Draw” are:

Existing Files - This is self-explanatory; your previously created files would be listed here,

Print - You can choose the page size you want when starting a new project,

Screen - This gives you choices for your monitor resolution,

Video - Lets you choose the type of video you want to create,



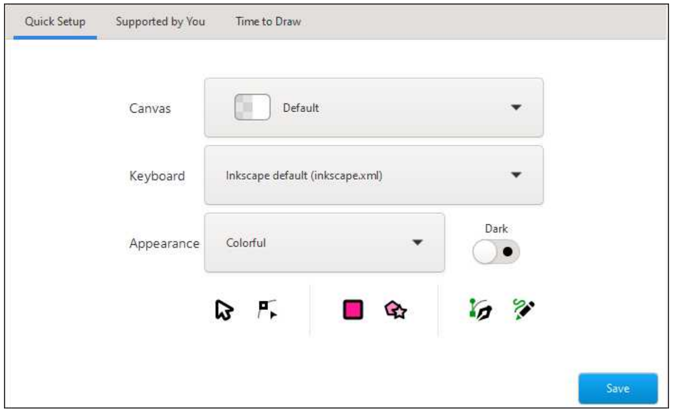
Recent Files
July2021CoverMaybe.svg
VeteranMarkerTrace.svg
NewTux.svg
June2021CoverMaybe.svg

☑ Show this every time

Social - This contains pre-formatted templates for items to be uploaded to social media sites like Facebook, Snapchat, LinkedIn, etc.,

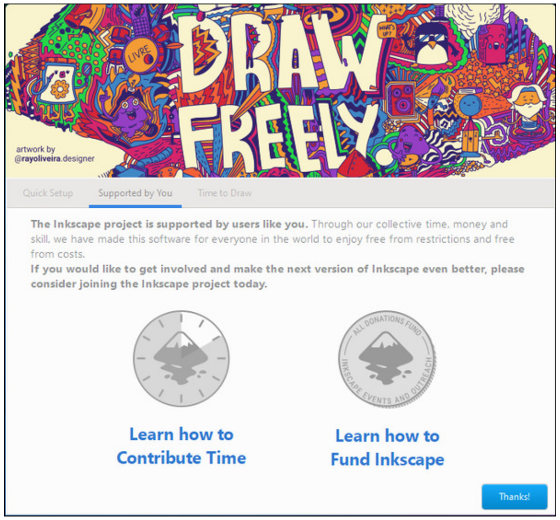
Other - This includes preformatted templates for icons and name tags.

Also, the look of Inkscape can be selected (Quick Setup). Choices are how you want your canvas to look, what keyboard you are using, and the appearance you want (including 6 choices of tool icons), and whether it should be dark or light.



Canvas: Default
Keyboard: Inkscape default (inkscape.xml)
Appearance: Colorful

Also in the Welcome Dialog is a tab named “Supported by You” which contains credits and links to Inkscape.org

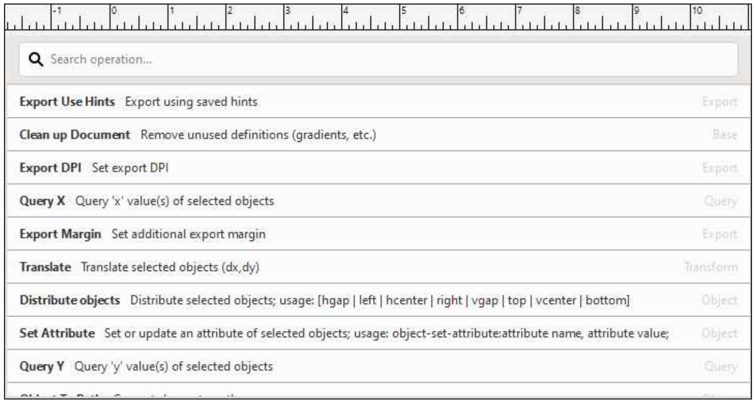


The Inkscape project is supported by users like you. Through our collective time, money and skill, we have made this software for everyone in the world to enjoy free from restrictions and free from costs.
If you would like to get involved and make the next version of Inkscape even better, please consider joining the Inkscape project today.

There’s also a checkbox to turn off the Welcome screen (in the Time to Draw tab).

Other improvements are:

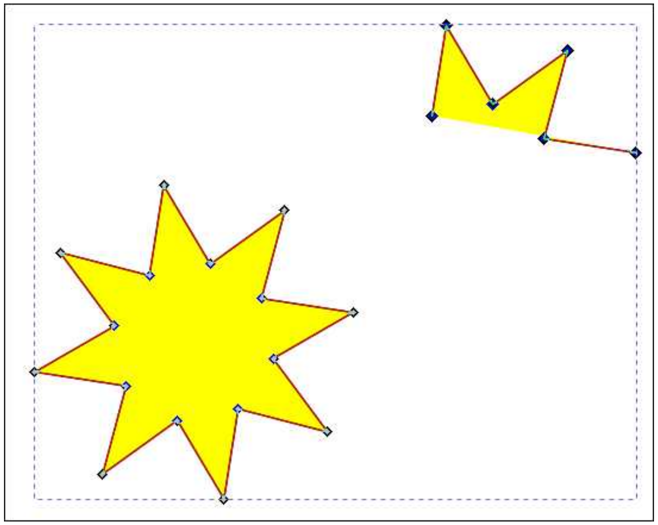
--- A **Command palette** that opens when the ? key is pressed which allows you to search and use many functions without having to use a keyboard shortcut or going through the menus.



Search operation...

Export Use Hints	Export using saved hints	Export
Clean up Document	Remove unused definitions (gradients, etc.)	Base
Export DPI	Set export DPI	Export
Query X	Query 'x' value(s) of selected objects	Query
Export Margin	Set additional export margin	Export
Translate	Translate selected objects (dx,dy)	Transform
Distribute objects	Distribute selected objects; usage: [hgap | left | hcenter | right | vgap | top | vcenter | bottom]	Object
Set Attribute	Set or update an attribute of selected objects; usage: object-set-attribute:attribute name, attribute value;	Object
Query Y	Query 'y' value(s) of selected objects	Query

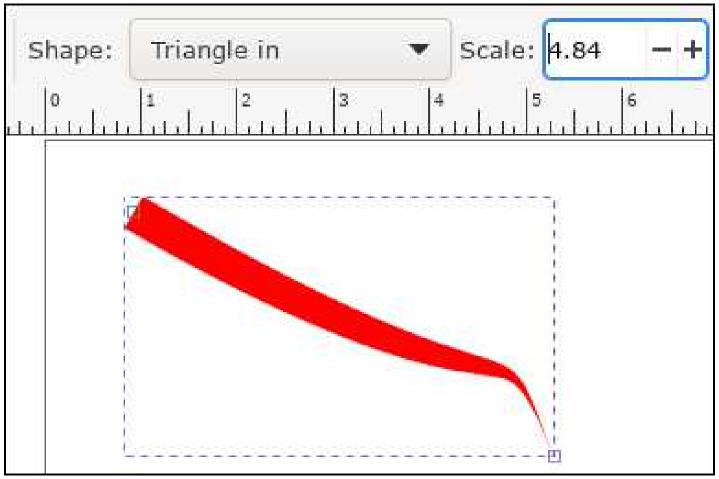
In the overlay that appears, a **search box** allows you to find any available command to execute on the whole drawing or selection. The list of available commands is currently restricted to those commands that have already been converted to 'actions'. Additionally, it includes the option to **import or open files** from Inkscape's document usage history. Since I hadn’t typed anything in yet, everything is there. I needed to search for a particular action.



--- It is now possible to copy, cut and paste parts of paths with the Node tool. These nodes can be inserted **into the original path, into a different path** or they can be **pasted as a completely new path**. I selected several nodes (below) and copied and pasted them into my drawing, but separately.

--- The **dialog docking system** has been rewritten, which resolves many issues with Inkscape's docked dialogs and allows you to dock dialogs on either side of the screen. I don’t ever dock any of them, so I didn’t try this one.

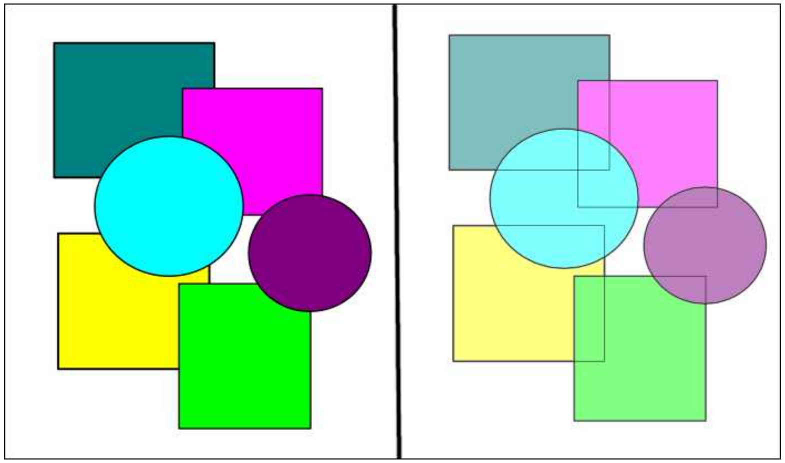
--- The Pen and Pencil tools feature a new '**Scale**' option to set the **width of paths** created with a “Shape” option other than “None” numerically. I did a line with the “Triangle Out” option, and if you select the Nodes tool, there is still a handle on the end to adjust the stroke width. However, there is now a numerical setting that you can access while you still have the pen/pencil tool selected.



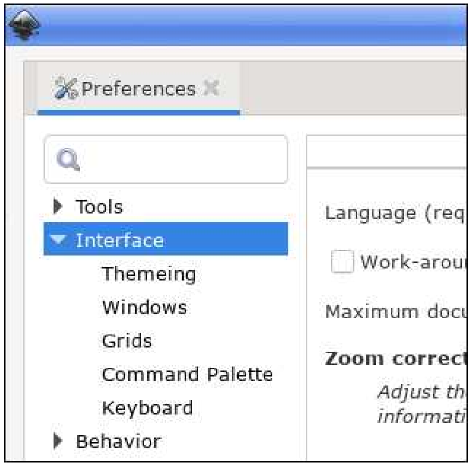
Shape: Triangle in

Scale: 4.84

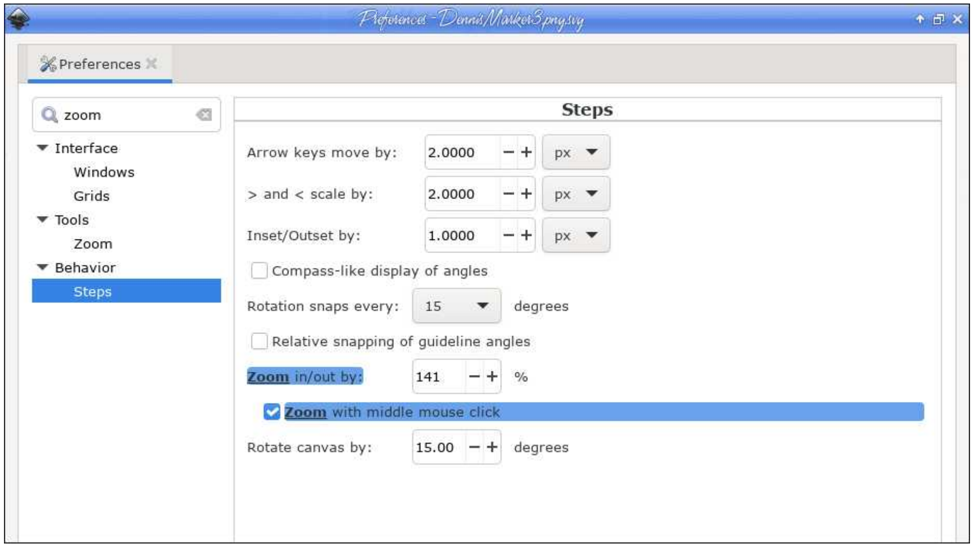
--- A new **Outline Overlay mode** that displays object outlines while also showing their real colors. You can see the difference here between Normal View and Outline Overlay View. For very detailed drawings I’m sure this would be very useful. These are in **View > Display Modes**.



--- The **Preferences options** are now easier to find by using the new search field



When you search with a particular term (zoom, for example), the window will show you every section in which you can find it.



Steps

Arrow keys move by: 2.0000 px

> and < scale by: 2.0000 px

Inset/Outset by: 1.0000 px

□ Compass-like display of angles

Rotation snaps every: 15 degrees

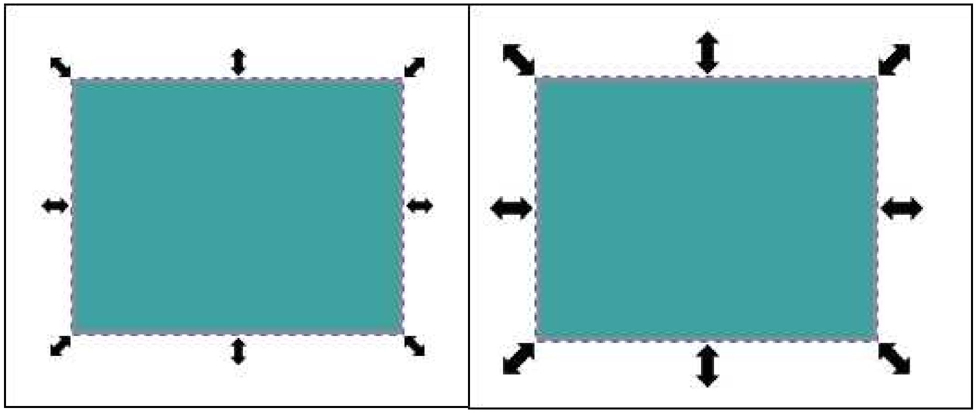
□ Relative snapping of guideline angles

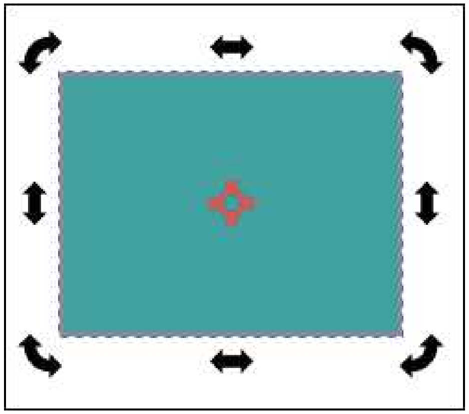
Zoom in/out by: 141 %

☑ Zoom with middle mouse click

Rotate canvas by: 15.00 degrees

--- The **maximum handle size has been increased**, so you can enlarge them to a more comfortable size from **Edit > Preferences > Interface: Handle size**. The handles on the left are size 4, and those on the right are size 8. (This may help some of us whose eyes aren't as sharp as before.) top, right





The **rotation center** handles have been made more visible. (I always had to search for the little plus sign.)

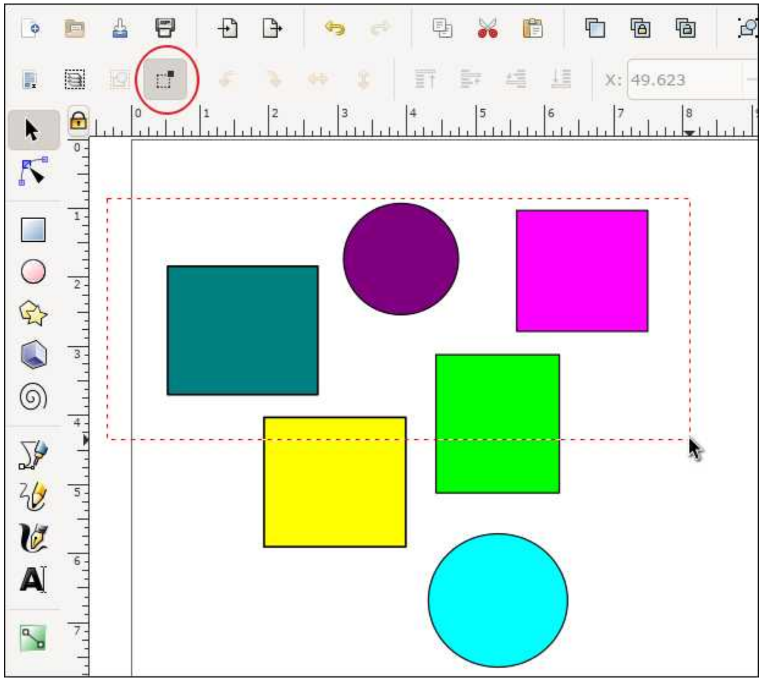
--- When pasting a copied object, Inkscape can now paste it directly on top of the currently selected object by default. You can copy an object, select a different object, and when you paste, your copied object will be pasted on top of the one you selected. The feature can be disabled, if you wish.

--- A **new selection mode** for the selection tool was added, which can now select every object that is either **within the box or that touches its boundaries**. The mode can be activated by pressing the **corresponding button** in the Selector tool's control bar. On canvas, you can see that the mode is activated by the red color of the selection box while dragging. When not activated, the selection box is black (next page, top left).

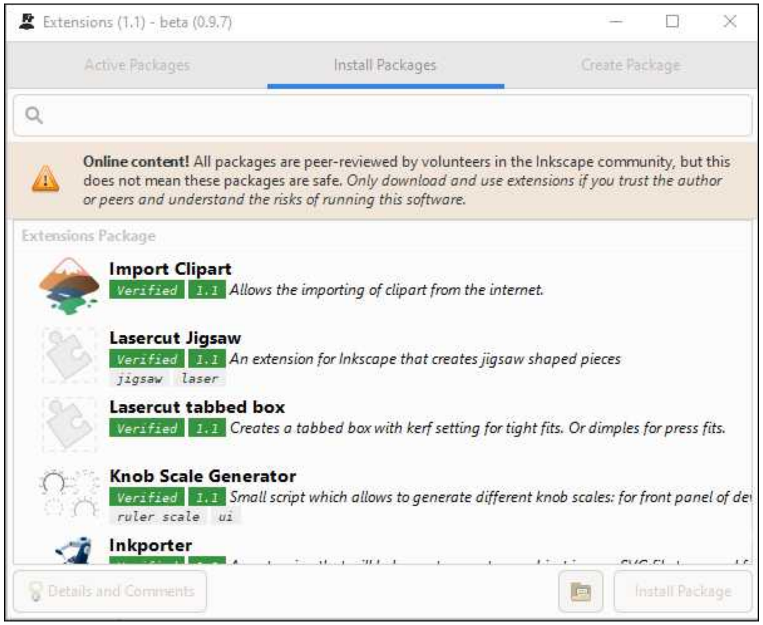
When I released the mouse button, all shapes except the bottom circle were selected.

--- An extension for updating extensions and installing additional extensions, called the Extension Manager (currently in beta stage). I haven't tried installing anything yet (next page, bottom left).

To learn more, see the full release notes for Inkscape 1.1. I'm sure you can find something else interesting!



New Selection Tool



Extensions (1.1) - beta (0.9.7)

Online content! All packages are peer-reviewed by volunteers in the Inkscape community, but this does not mean these packages are safe. *Only download and use extensions if you trust the author or peers and understand the risks of running this software.*

Extensions Package

Import Clipart
Verified 1.1 *Allows the importing of clipart from the internet.*

Lasercut Jigsaw
Verified 1.1 *An extension for Inkscape that creates jigsaw shaped pieces*
jigsaw laser

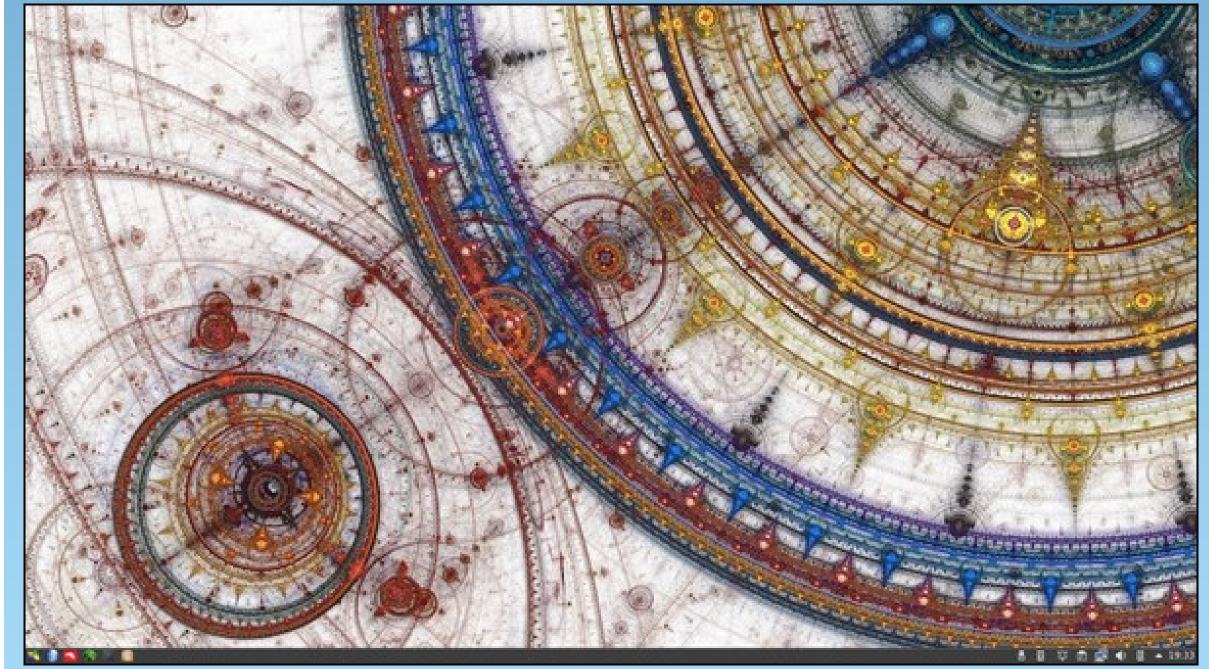
Lasercut tabbed box
Verified 1.1 *Creates a tabbed box with kerf setting for tight fits. Or dimples for press fits.*

Knob Scale Generator
Verified 1.1 *Small script which allows to generate different knob scales: for front panel of de*
ruler scale ui

Inkporter

Extensions Manager

Screenshot Showcase



Posted by luikki, July 2, 2021, running KDE.

Audacity: Now Considered Spyware

by Paul Arnote (parnote)

Just when you thought it was safe to go back in the water …

Over the last couple of months, the FreeNode IRC network has detonated or imploded (take your pick of which word to use, depending on your point of view), as we reported on last month. FreeNode was the IRC "home" of many FOSS projects.

Prior to that, we were embroiled in (and reported on) another "scandal" where the new owners of LastPass made the popular password manager a subscription-based service, after being a free service ever since its inception.

FOSS projects have taken a beating in 2021, and the year isn't but two-thirds done yet.

Now, another FOSS project is causing a "scandal." The project (which you are most likely already familiar with), the open source multi platform sound editor Audacity, was acquired by Muse Group on May 4, 2021. This Russian-based company is the same one that controls the open source music notation program known as MuseScore. On July 4, 2021, Muse Group published a new "desktop privacy notice" where data is collected from the end user's computer, and that data is transmitted back to servers run by Muse Group. Once there, that data is retained and may be handed over to "competent law enforcement agencies" upon request. You can read the entire updated "privacy" policy here. There are other "contentious" parts of the new "privacy" policy, as well, but this particular part was exceptionally disturbing.

For what it's worth, the new "privacy" policy appears to be a shorter version of the privacy policy that the Muse Group has applied to MuseScore. However, MuseScore doesn't have even a fraction of the number of users as Audacity, which is probably why it has flown under the radar. Audacity is one of the most popular FOSS programs on the planet, hence the outrage.

Whoa! Whoa! Whoa! Say WHAT?!

As you might imagine, the open source community reaction has been swift and very, very negative. Muse Group's data collection, and the subsequent "phoning home" with that collected data, is leaving many in the open source community feeling betrayed. The last thing open source users … nay, any users … want is to be spied upon by a program that phones home with various data that, if taken in a certain way, may incriminate users when in fact nothing wrong has been done at all. Plus, in an era when user privacy is increasingly under attack, someone else trying to collect user data isn't going to be taken lightly.

Besides the data collection that has users up in arms, the new "privacy" policy is in direct violation of the GPL (the license under which Audacity is currently released) by "restricting" its use to users 13 years of age or older. The GPL prevents any restrictions of any kind, including age.

Almost immediately, there were many calls to fork Audacity. One GitHub user, Cookie Engineer, stepped forward to do just that. One of the first orders of business was to select a new name for the Audacity fork, since the name "Audacity" is trademarked and "owned" by Muse Group. The new fork will be called "Tenacity."

Another important issue with the fork was to go through the code and remove all the telemetry/data collection and the "phone home" reporting routines. According to the Tenacity page on GitHub, this has already been accomplished.

The "discussion" section of the Tenacity page on GitHub is full of other considerations for the fork. One is whether to continue using the same wxWidgets framework that Audacity uses, or whether to port it to the Qt or GTK3 framework.

Other concerns were expressed by Cookie Engineer from the outset. He acknowledged that he would need help to maintain the fork, and that a team of coders would need to join him in the effort to maintain the fork. He also expressed a need for someone to build the fork for the Windows OS, MacOS and BSD, since he alone would not be able to provide those binaries.

Stay tuned. Source code for the Tenacity fork is already posted on the Tenacity GitHub page. While the fork is in the early stages, it shouldn't be long before Tenacity is available in most Linux distribution's software repositories. Tenacity is coming from a fairly stable code base, since Audacity has been around for over 21 years. Audacity was originally released in May, 2000 as version 0.8, by Dominic Mazzoni and Roger Dannenberg at Carnegie Mellon University.

The current version of Audacity (3.0.2) in the PCLinuxOS repository is free of the telemetry/data collection and "phoning home" privacy violations, so there's no need to uninstall it from your computer just yet. Newer versions won't be so lucky. Expect to see Audacity to be replaced (probably with Tenacity) in the near future on your PCLinuxOS installation.

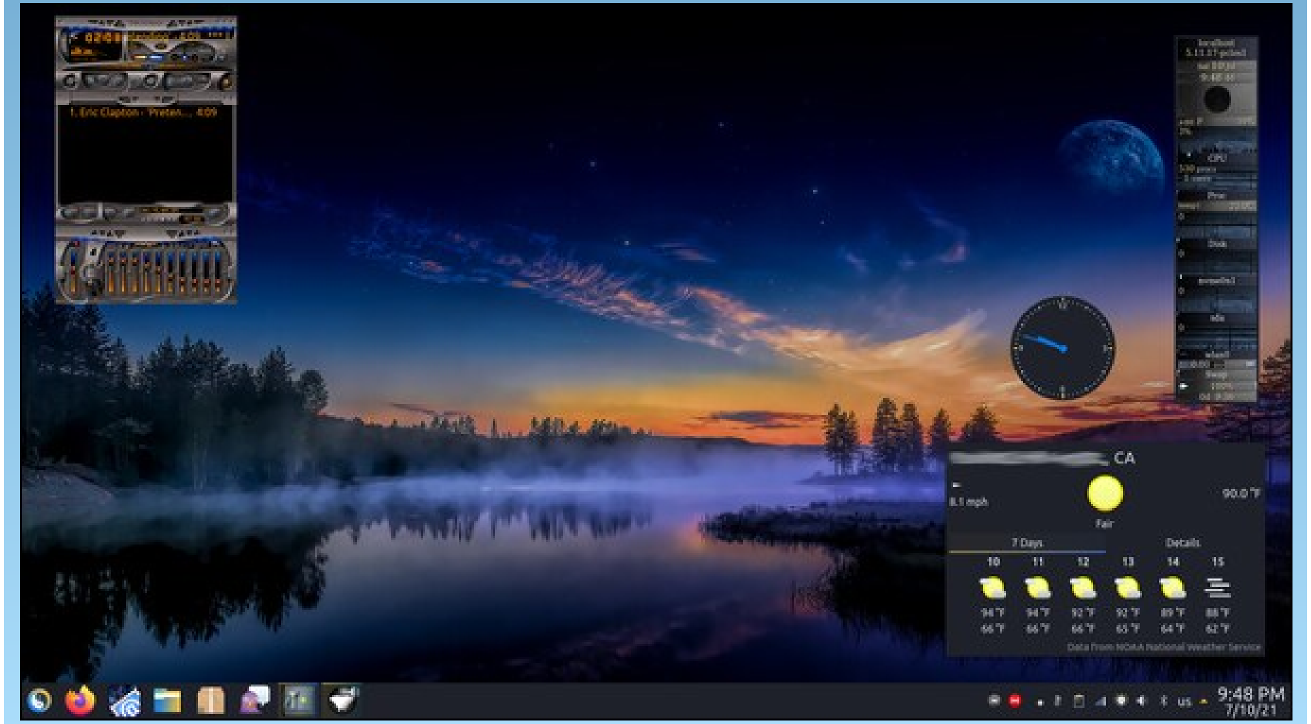
Even if Muse Group were to back away from their telemetry/data collection scheme, it's now too late. User trust has been irreversibly destroyed. Users will wonder in the back of their minds if they might again attempt such shenanigans, or if they might have quietly slipped the telemetry/data collection/phone home code back into a subsequent release. And that doesn't even address the GPL violation of releasing software with NO restrictions, including age.

Just as with FreeNode and LastPass, user confidence and trust has been shattered, and it could very well spell the end of Audacity's reign as the best and most used FOSS sound editor. It is sad, indeed.

Thanks for the memories, Audacity. You served us well. Now, it's time to move on, away from underhanded owners collecting untold amounts of user data. You don't destroy the boat that has delivered you to the shore, in a manner of thinking, and that is exactly what Muse Group has done to the users of Audacity. With Audacity, the FOSS community delivered a high quality product, built upon sound FOSS pilings. It's time to say goodbye to Audacity, and hello to Tenacity … or whatever else comes along to replace its niche in the software landscape.

LAST MINUTE UPDATE: *Just as this issue of The PCLinuxOS Magazine was "going to press," Muse Group has changed course and decided to NOT put telemetry and data collection code into Audacity, due to the negative publicity and rabid backlash from users. Only time will tell if this change-of-course lasts. Their willingness to collect the data in the first place, and to turn it over to law enforcement on a whim, is still very concerning.*

Screenshot Showcase



Posted by tuxlink, July 11, 2021, running KDE.

Linuxera: A Former Forum Admin Could Use Our Help

by Meemaw

Back in 2006, when I registered on the forum, there were some wonderful people here! Texstar was here of course, along with some that are still here: The Heat Exhausted Cranky Zombie, davecs, JohnW_57, wayne_1932, tuxalish and many more who are no longer around. Others registered shortly after I did, including parnote. In the fifteen years since I started visiting, I have come to feel that many of these people, whether I had ever met them or not, were good friends. We’ve shared many ups and downs.

A very knowledgeable lady whose handle was Linuxera was here as well. She was an admin even then, and helped to keep us all in line. She was also a tester, and experimented with creating ISO’s of Enlightenment, and talked me through creating a backup ISO of my system years ago. She had lived in many places, including Florida and Oregon, but moved to Alabama a few years ago. Her first house in Alabama was really close to a river area that had some flooding, so she moved a bit north where the river wasn’t in her backyard. Sometime after 2012, for reasons unknown to me, she deleted her user profile in the forum.

We’ve chatted and emailed sporadically since then. I found out her name is Cindy Solis. She is an Air Force veteran, and is now eligible for Social Security. She’s shared photos of her chickens and her dog and how she cleaned up the property where she lived, and I shared photos of my area and some of the activities I am involved in.

In May, 2021, I got a short email from her. The email subject line read “Please post this link on fb, twitter, social media”, and in the body, she said, “Forever indebted. VA community services wants me to drive 60 miles for appointments. I can barely walk still. love you all/” The GoFundMe link outlined the circumstances of her stroke!

After texting her (and later, speaking with her), I posted the link on the forum and on Facebook asking for donations to her GoFundMe fundraiser. She says she is doing much better now, only having some weakness in one leg and a few memory problems. She lives in such a small town that they had to Life Flight her to a larger hospital. The VA Center she goes to for medical care is 60 miles away, so driving that is a problem. I helped her a little (I hope), giving her the VA form for Travel pay that my husband used when he went to the VA. I hope she can use it as well.

If you visit GoFundMe, you will see that her son Jason set up the fundraiser. He explains that since he has health issues of his own, he can’t travel to her home to care for her and this was one way he could help.

If you’re able, I hope you will donate.

Short Topix: Microsoft? Has Its Own Linux??

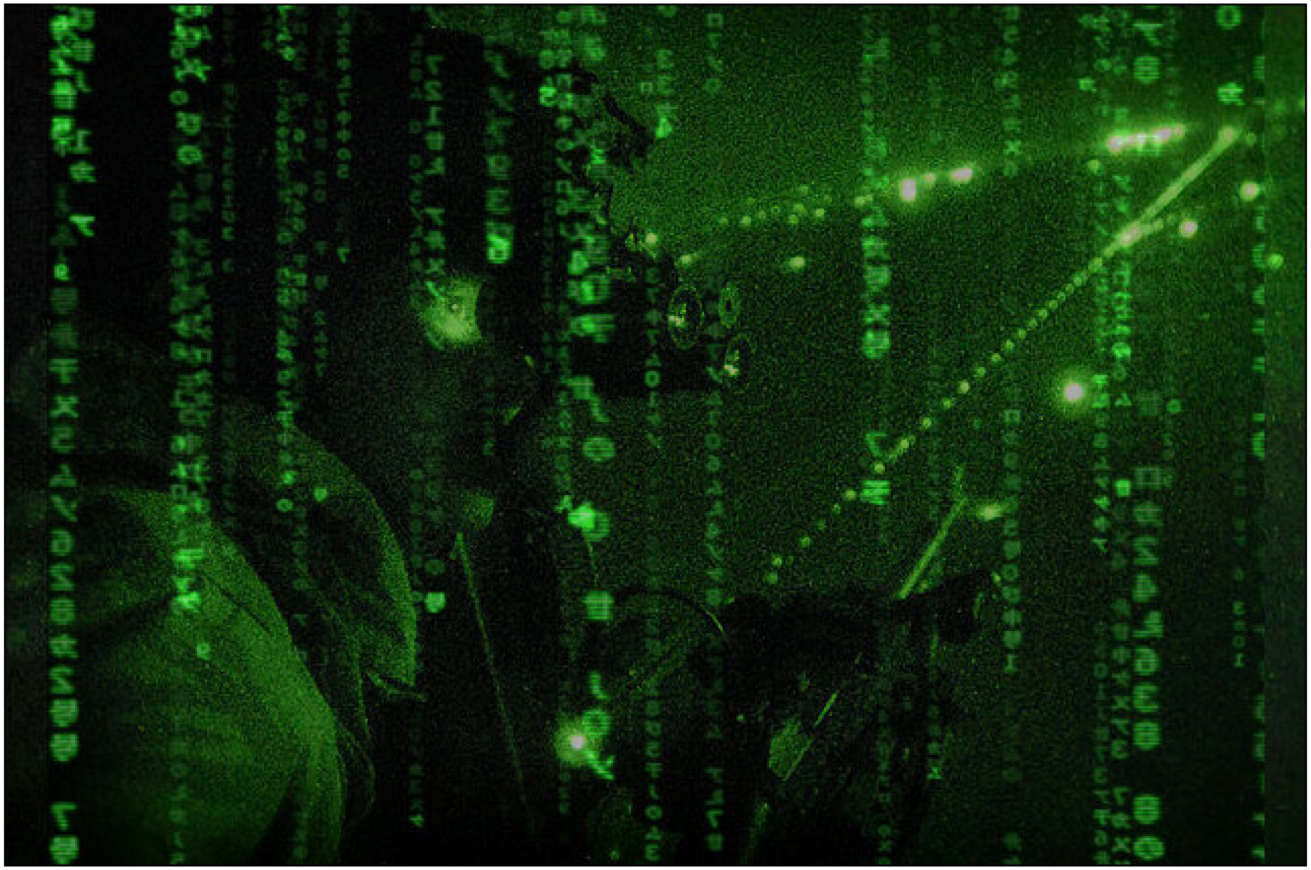
by Paul Arnote (parnote)

As frequently as assaults on your privacy happen, I figured I probably needed to make something about them a regular part of the Short Topix column. I seem to be reporting on privacy intrusions on a monthly basis here, so we might as well have a regular place to put them. So, below is the inaugural appearance of "The War On Your Privacy" portion of this monthly column.

To better define the scope of what I'll be covering in this section of my monthly Short Topix column, it'll be pretty much restricted to data breaches and other intrusions on your privacy. Other news items announcing ways to protect your privacy will, when reported on, be given their own section of Short Topix as I've always done.

The War On Your Privacy Monthly Update

AN ARTICLE ON TECHRADAR PRO reports that 700 million LinkedIn records have been scraped from the career networking site, and are being offered for sale on an underground hacking forum. This follows two months after 500 million records from the career networking site were sold off in a similar manner. The latest LinkedIn breach was initially reported by the VPN review site, PrivacySharks. LinkedIn is still investigating the issue, but their initial analysis points to only information from public-facing pages being included, and that no private information of users was compromised.



Tom Burt, Microsoft Corporate Vice President of Customer Security & Trust, reported in **TESTIMONY TO THE UNITED STATES HOUSE COMMITTEE ON THE JUDICIARY'S HEARING** on "Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power" that Microsoft receives between 2,400 and 3,500 requests from federal law enforcement officials ***per year***, or between seven and 10 per day, for Microsoft users' information.

Excerpted from Burt's written testimony:

Traditionally, secrecy was the exception. In recent years, law enforcement has turned that exception on its head, developing a practice of reflexively asking to keep even routine investigations secret. Providers, like Microsoft, regularly receive boilerplate secrecy orders unsupported by any meaningful legal or factual analysis.

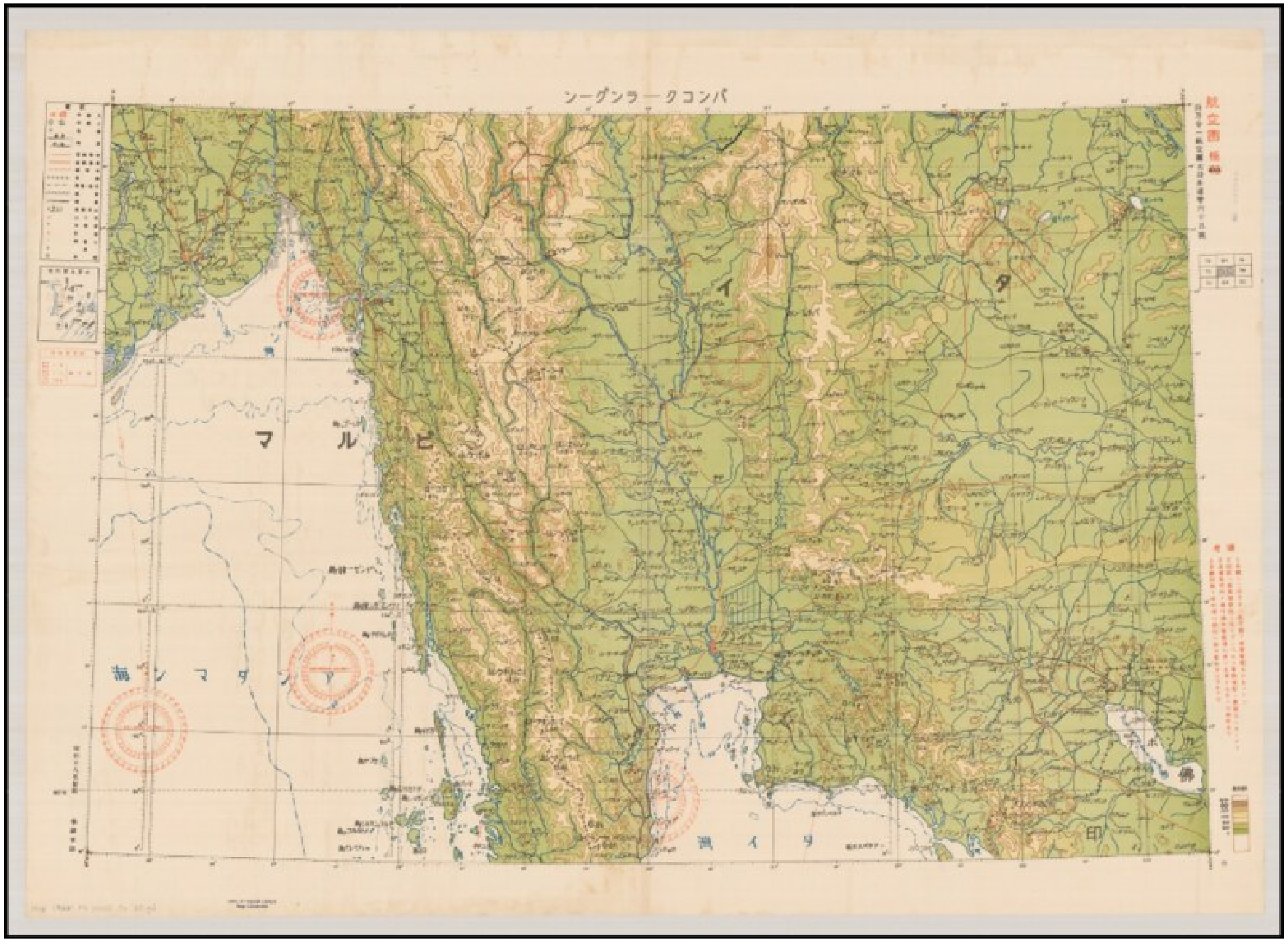
Microsoft does not simply comply with such demands without question. We review them closely to protect our customers' interests. Some of the demands Microsoft received were legally deficient and we did not comply. In other cases, we have challenged — through negotiation or litigation — the orders. This includes secrecy orders approved by courts where the account holder was not a *target of the investigation but a victim; where the investigation related to just one email account belonging to a large, reputable organization — a company, government, or school — and there was no allegation that the organization itself or its leadership was suspected of wrongdoing; where the government was engaged in discovery negotiations with an organization under investigation, and then secretly demanded the very same records from us to evade a dispute over privilege and the extent of discovery; and even where the owner of the target account consented to the search.*

You can read Burt's full written testimony before the committee hearing here (PDF). It is QUITE eye-popping. And you wonder why people don't trust their own governments to do the right thing.

A JANUARY ATTACK ON MICROSOFT EXCHANGE SERVERS that spanned into February and early March of this year, has been tracked to a Chinese government-sponsored hacking group by U.S. officials and several U.S. allies, according to a report from the Associated Press. According to a previous article in March from the AP, "the hackers grabbed data, stole credentials or explored inside networks and left backdoors at universities, defense contractors, law firms and infectious-disease research centers." Concerns are especially high among those worried about intellectual property theft, hospitals, financial institutions and managed service providers who host multiple company networks.

WWII Gaihōzu (Japanese Imperial Maps) Rediscovered

After the end of World War II, American (and other Allied forces) captured thousands of military maps from the Imperial Japanese armed forces. These maps weren't just of Japan, either. These maps were from all over Asia, including Korea, China, USSR, Burma, Thailand, and many of the Pacific Islands.



Realizing their value, the U.S. Army sent these maps … called gaihōzu … back to the U.S. for safe keeping. But, because of their intelligence and tactical value, it was decided that all of these maps shouldn't be stored all in one place. So, they sent them to libraries scattered all around the U.S., and there they sat, gathering dust and forgotten.

That is, until a former Stanford graduate student working on a Master's dissertation about the ancient Chinese Han dynasty started asking around about some rumored maps of old Asia, according to an article on National Geographic. Her search led to their rediscovery.

Sometimes, especially early on, Japanese cartographers would use and appropriate maps made by the local indiginous people. But, as time went on, they discovered the maps weren't detailed enough to suit their needs. So, Japan sent out teams of surveyors to create more detailed maps. The other countries and regions these surveyors were mapping weren't always that "thrilled" about the presence of the Japanese surveyors. In fact, at one point, an entire Japanese surveyor team simply "disappeared."

These detailed maps now hold a lot of historical significance. It offers a fascinating window on the history of Asia, as well as World War II. You can view collections of these historical maps by visiting the Gaihozu Digital Archive, and the Gaihozu: Japanese Imperial maps collection at the Stanford library.

Microsoft? Has Its Own Linux??

Are you sitting down? If not, take a moment, find a chair, and plant your backside in it. I wouldn't want anyone falling out and injuring themselves.

Microsoft has its own version of Linux, called CBL-Mariner. The "CBL" stands for Common Base Linux.

There. I said it. It has actually happened.

Are you still vertical? Do you need to catch your breath?

After years of declaring Linux a cancer and doing everything in its power to eliminate Linux from the computing landscape, Microsoft has its own version of Linux. [GASP!!!!]

Don't expect to find it too useful, though. CBL-Mariner is a lightweight Linux server. In fact, no ISO currently exists of CBL-Mariner, but you can download the source files from GitHub and build it yourself. To build it, you have to be running Ubuntu 18.04, though (although there are reports of it being successfully built on even more recent versions of Ubuntu). Plan on the build process taking you just under an hour to complete.

There is no desktop environment. Just a plain old command line. It's geared towards powering "the cloud." Microsoft released it without any fanfare. It just took people quite a while to notice it. Built for its own internal use, CBL-Mariner's first commit on GitHub was in July 2020. It literally took a full year for most people to sit up and take notice.

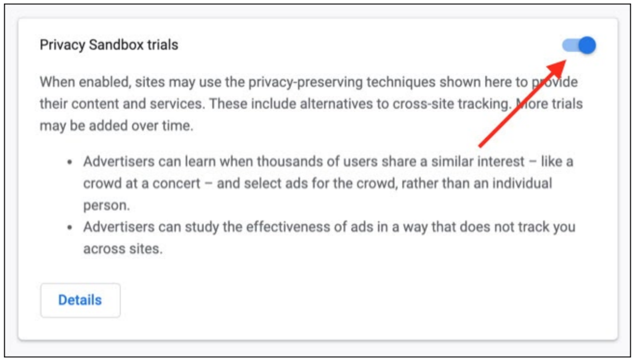
Don't get your hopes up, though, as TechRepublic's Jack Wallen did. No, Microsoft isn't rebasing Windows on Linux (although that should have happened YEARS ago). ZDNet's Steven J. Vaughan-Nichols also seems quite giddy about CBL-Mariner. Vaughan-Nichols gives a good summary of just what CBL-Mariner's role is.

Still, for those of us who have been around computing for a significant amount of time, this revelation is shocking and unexpected. Miracles will never cease!

Get The FLoC Outta Here!

If you haven't heard by now, Google is supposed to be moving away from the dreaded cookies that identify individual users as they move about the internet. Google plans to replace cookies with FLoC, which stands for "Federated Learning of Cohorts." Here's what EFF (Electronic Frontier Foundation) says to explain FLoC:

> *FLoC runs in your browser. It uses your browsing history from the past week to assign you to a group with other "similar" people around the world. Each group receives a label, called a FLoC ID, which is supposed to capture meaningful information about your habits and interests. FLoC then displays this label to everyone you interact with on the web. This makes it easier to identify you with browser fingerprinting, and it gives trackers a head start on profiling you.*



Privacy Sandbox trials

When enabled, sites may use the privacy-preserving techniques shown here to provide their content and services. These include alternatives to cross-site tracking. More trials may be added over time.

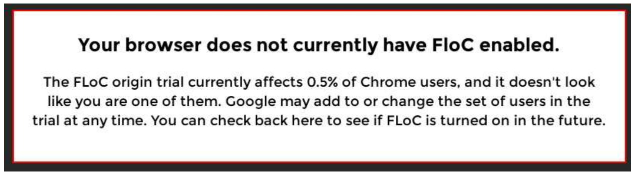
- Advertisers can learn when thousands of users share a similar interest – like a crowd at a concert – and select ads for the crowd, rather than an individual person.
- Advertisers can study the effectiveness of ads in a way that does not track you across sites.

Google is now trialing FLoC on about 0.5% of random Google Chrome users. To see if you are one of the "lucky" Google guinea pigs, under the hamburger menu, go to Settings > Privacy and security > Privacy sandbox. If you don't see this item, you are not a part of Google's Frankenlab experiments.

Simply turn the slider in the upper right corner to the OFF position to opt out of being one of Google's test subjects. Don't think, however, that you cannot or will not be added to further rounds of testing later, so check back often. Once Google goes "live" with FLoCs and lets its monster out of its cage, don't hold your breath about being able to opt out of using the new tracking technology.

While Google claims that FLoC will protect user privacy far better than cookies, there are many critics of the use of FLoCs. They say that in many ways, they are worse than cookies. Leave it to Google to come up with something worse than cookies that serves their [greedy] pursuit of advertising dollars.

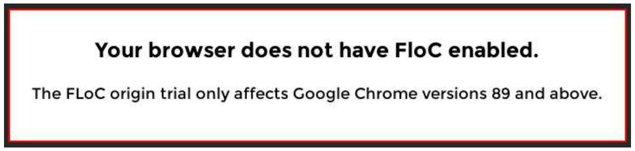
Thankfully, you are not alone in your concerns. The EFF is leading the charge against FLoCs, along with most other "technologies" that track users and compromise their privacy. They even have a special website, named **Am I FLoCed?**, that will check to see if you are being tracked by the Google FLoC of geese.



Your browser does not currently have FloC enabled.

The FLoC origin trial currently affects 0.5% of Chrome users, and it doesn't look like you are one of them. Google may add to or change the set of users in the trial at any time. You can check back here to see if FLoC is turned on in the future.

Google Chrome



Your browser does not have FloC enabled.

The FLoC origin trial only affects Google Chrome versions 89 and above.

Firefox

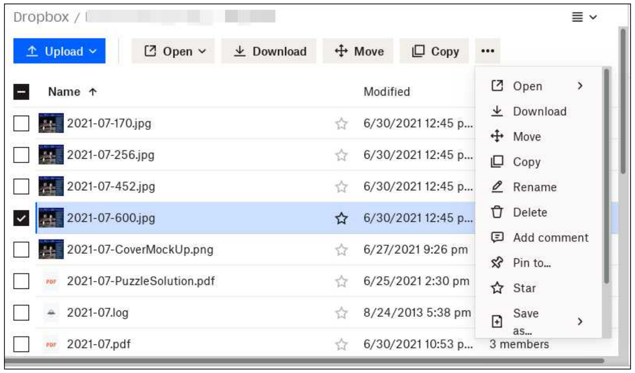
If you connect to the **Am I FLoCed?** website in Chrome, you will see the top message above displayed in Chrome. Out of curiosity, I tried the website in Firefox, and I got the message in the bottom image above displayed. The website goes on to give a good, easy-to-understand explanation of the new FLoCs, and how they might compromise your privacy.

Google is trialing FLoC **ONLY** in Google Chrome, and it has not spilled over to any other browser, including any of the Chromium variants (Brave, Edge, Chromium, etc.). No other browser maker (like Mozilla) has come out in support of Google's new FLoC tracking.

If you ever needed a/another reason to hate Google and/or ditch Google Chrome, you might want to pay attention. FLoC represents a direct assault on your privacy, spearheaded by Google. If this isn't enough to persuade you of Google's evil intent, then nothing ever will and you deserve what you get.

Dropbox Adds New Features, Capabilities

Citing the explosion in WFH (working from home) over the past 15 months brought on by the COVID pandemic, the Dropbox team has added some new features. Most of these new features are available to both paid and free Dropbox users, albeit only on the Dropbox web page, and (sadly) not from your Dropbox directory on your computer.



	Name ↑		Modified	
□	2021-07-170.jpg	☆	6/30/2021 12:45 p...	
□	2021-07-256.jpg	☆	6/30/2021 12:45 p...	
□	2021-07-452.jpg	☆	6/30/2021 12:45 p...	
☑	2021-07-600.jpg	★	6/30/2021 12:45 p...	
□	2021-07-CoverMockUp.png	☆	6/27/2021 9:26 pm	
□	2021-07-PuzzleSolution.pdf	☆	6/25/2021 2:30 pm	
□	2021-07.log	☆	8/24/2013 5:38 pm	
□	2021-07.pdf	☆	6/30/2021 10:53 p...	3 members

Still, here are some of the new features you are apt to see in Dropbox. First, Dropbox will allow you to convert between JPG, PNG and PDF file formats without having to leave the Dropbox site, and without having to first download the file and then manually convert them on your computer, before re-uploading them to Dropbox. There are plans to add video file conversion, as well, according to the Dropbox folks. They have also dramatically improved camera uploads to Dropbox, making it easier to use Dropbox to share images and files with family and friends. The new Dropbox Passwords feature allows you to store, sync and share your passwords between devices. It also contains support for debit and credit card numbers. The "Suggested Folders" feature helps users add and share the right content with the right people, but is available only to those Dropbox users with a paid subscription.

Personally, some of these new features sound pretty enticing and will be welcomed by many Dropbox users. However, some of these new features sound like a security nightmare in the making. I, for one, would be hesitant to store my passwords and debit/credit card numbers in my Dropbox account.

The risk, in the event of a data breach, is just too great.

Now … if only Dropbox would increase the storage space allotted to Basic (free) users beyond the 2GiB of space that they've offered since Day One.

Google Maps Leads Users To Potentially Fatal Hiking Trail

Ben Nevis is the highest mountain in Scotland, standing 4,412 feet (1,345 meters) tall. As mountains go, it's no Mt. Everest, but it's still fairly tall. And, as with many mountains, it can be deadly to hikers and mountaineers.

The United Kingdom conservation charity John Muir Trust and Mountaineering Scotland, the national representative body for mountaineering, hillwalking, climbing, and snow sports touring, has specifically warned that a route provided on Google Maps, which leads hikers to a parking lot at the head of Glen Nevis, could be putting people at risk. Google Maps can proceed to display a dotted line to show a path to the top of the mountain, one which would be difficult for even the most experienced mountaineer to follow.

Heather Morning, Mountaineering Scotland's Mountain Safety Adviser, said in a statement released by the conservation charity, "For those new to hill walking, it would seem perfectly logical to check out Google Maps for information on how to get to your chosen mountain. But when you input Ben Nevis and click on the 'car' icon, up pops a map of your route, taking you to the car park at the head of Glen Nevis, followed by a dotted line appearing to show a route to the summit."

Morning added, "Even the most experienced mountaineer would have difficulty following this route. The line goes through very steep, rocky, and pathless terrain where even in good visibility it would be challenging to find a safe line. Add in low cloud and rain and the suggested Google line is potentially fatal."

Since the criticism, Google has changed the driving instructions to get to Ben Nevis to take visitors to the mountain's visitor center, where they can discuss with park personnel the best route to take to climb or hike Scotland's highest mountain.

PCLinuxOS Short Topix Roundup

WHO BETTER TO DESIGN NEW AI COMPUTER CHIPS THAN AI? An article at WIRED highlights just that approach. Computer chips, often smaller than a fingernail, contain billions of components. Each and every decision made on the arrangement of those components has the potential to affect the speed and efficiency of the resulting chip. So, to place a billion transistors on a small computer chip, who better to do it than AI? While attempts to have computers help design computer chips in the past have fallen short, new advances in AI have made such matters within reach.

Remember when you were told that the data being collected from your cell phone was being anonymized? Well, you were being lied to, even if it's a lie by omission. According to an article on Vice, they are **FAILING TO TELL YOU ABOUT AN ENTIRE INDUSTRY THAT OPERATES IN THE SHADOWS**, and who's sole business model is to collect the unique cell phone ID and mobile advertising IDs produced by various apps (called MAIDs), and linking them to personally identifiable information. The article, to say the least, is eye opening and quite disturbing.

According to an article that appeared on Reuters, **THE GERMAN DATA PROTECTION OFFICER GAVE MINISTRIES UNTIL THE END OF THE YEAR TO CLOSE THEIR FACEBOOK PAGES**, after discovering that Facebook had failed to comply with German and European Union privacy regulations. Commissioner Ulrich Kelber said it was impossible to run a fan page in such a way that followers' personal data was not transmitted to the United States. Under EU law, personal data can only leave the EU for a jurisdiction with equivalently strict data protection rules, something that is not the case for the United States.

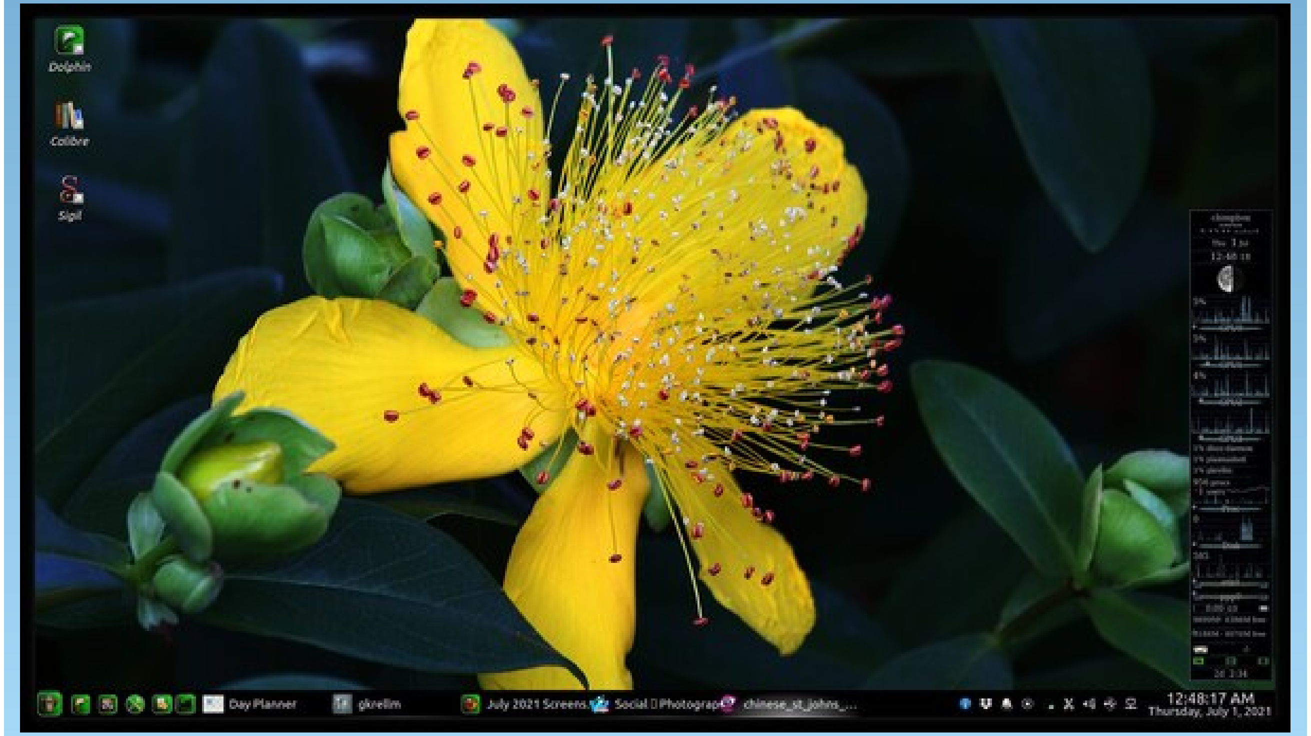
An article on Lifehacker **LISTS SOME OF THE MORE NOTABLE CHANGES IN FIREFOX 90**. Those include the ability to store credit card numbers, SmartBlock 2.0 working with Facebook to block the tracking Firefox users across the web, and the removal of the ability to download from FTP servers via a FTP.

JustTheNews published an article describing how Erik Finman, the youngest Bitcoin millionaire, has **CREATED THE FREEDOM PHONE, WHICH PROTECTS USERS' PRIVACY WHILE PROMOTING FREE SPEECH AND PREVENTING CENSORSHIP**. Built on top of a version of Android that has been “de-Googled,” it even has its own app store.

Privacy activist Edward Snowden, in an interview with The Guardian, warned that no mobile phone is safe, considering the revelations about the clients of NSO. He has **CALLED FOR A SPYWARE TRADE BAN** in the wake of the NSO revelations. NSO Group manufactures and sells to governments advanced spyware, branded as Pegasus, that can secretly infect a mobile phone and harvest its information. Emails, texts, contact books, location data, photos and videos can all be extracted, and a phone’s microphone and camera can be activated to covertly record the user.

Now this one is a bit funny. A lot of attention was being paid to Amazon founder and former CEO Jeff Bezos as he made his 10 minute flight into space aboard Blue Origin’s inaugural crewed flight. But the best part of the story (it was widely reported, and I saw it on Gizmodo and Reuters) may have been from Oliver Daemen, the 18 year old from the Netherlands. **He not only MADE HISTORY AS THE YOUNGEST PERSON TO GO INTO SPACE, BUT HE ALSO MADE HEADLINES FOR SOME “SMALL TALK” HE MADE WITH BEZOS**. He told Bezos that he had never bought anything off of Amazon. Bezos’ response was as priceless as it was true: “Oh, wow, it's a long time ago I heard someone say that.” Additional history was made on the flight, with 82 year old female pilot Wally Funk becoming the oldest person to fly into space.

Screenshot Showcase



Posted by The CrankyZombie, July 1, 2021, running KDE.

Streaming From PCLinuxOS To Your Smart TV

by Agent Smith (Alessandro Ebersol)

Watching DVDs these days has become an exercise in patience. Either the new smart TVs no longer have composite video inputs, or the DVD players are broken, and, many times, it doesn't even pay to have them repaired. But for those who have a reasonably sized DVD collection (as I do), it is not worth getting rid of them, after all, they are like books, physical pieces of artistic content that belong to you. Yes, I will still write about the war on physical media, but in the meantime I will give you a tip on how you can watch your entire DVD collection on your Smart TV with the help of PCLinuxOS.

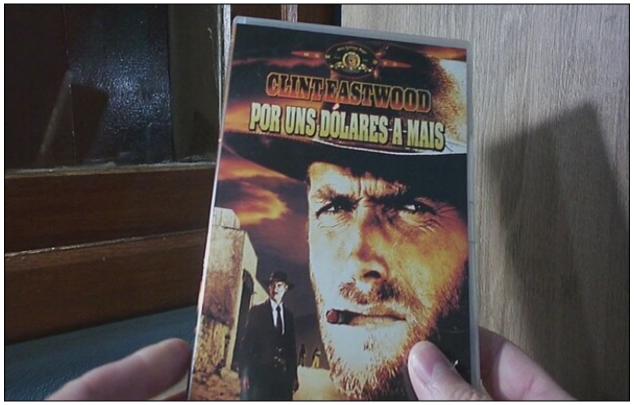
Let's get to the ingredients.

To make this tip work, you will need the following programs on your PCLinuxOS computer:

- Darkhttpd
- Handbrake

On the Smart TV side, it should be able to install a Firefox-derived web browser (depending on your Smart TV's manufacturer).

I wanted to watch a DVD on my Smart TV...



For A Few Dollars More, a classic from Sergio Leone

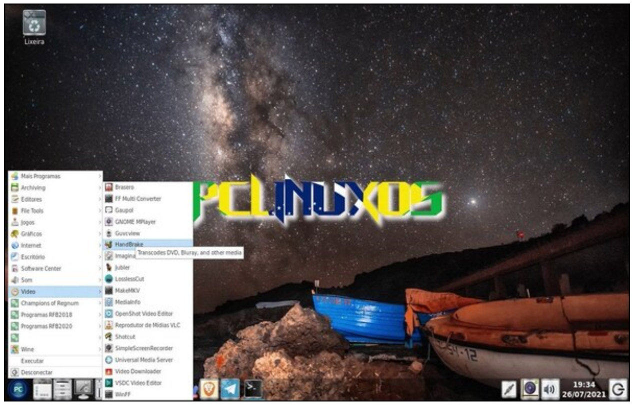
Yes, my need is what moved me to get a solution to this problem.

I had already tried the PS3 media server, the Universal Media Server (UMS), without success.

Then I remembered that Firefox and its derivatives can run media files from a web server without downloading the media file. This detail became the solution for me.

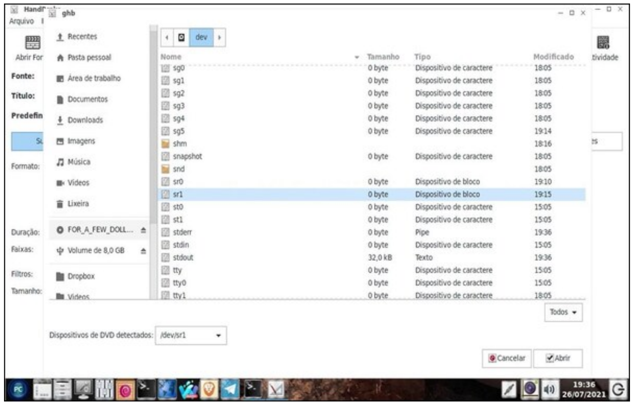
I loaded the DVD on my desktop PC with PCLinuxOS

Now, after you have loaded the DVD into your computer, the next step is to run Handbrake.



Handbrake is in the Video section of the programs menu

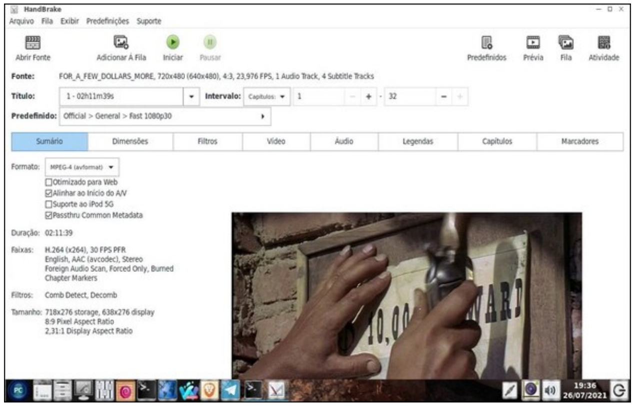
When running Handbrake, choose Open Source, navigate to the DVD drive and indicate the DVD disc as the source that will be transcoded.



Nome	Tamanho	Tipo	Modificado
sg0	0 byte	Dispositivo de caractere	18:05
sg1	0 byte	Dispositivo de caractere	18:05
sg2	0 byte	Dispositivo de caractere	18:05
sg3	0 byte	Dispositivo de caractere	18:05
sg4	0 byte	Dispositivo de caractere	18:05
sg5	0 byte	Dispositivo de caractere	19:14
shm			18:16
snapshot	0 byte	Dispositivo de caractere	18:05
snd			18:05
sr0	0 byte	Dispositivo de bloco	19:10
sr1	0 byte	Dispositivo de bloco	19:15
st0	0 byte	Dispositivo de caractere	15:05
st1	0 byte	Dispositivo de caractere	15:05
stderr	0 byte	Pipe	19:36
stdin	0 byte	Dispositivo de caractere	15:05
stdout	32,0 kB	Texto	19:36
tty	0 byte	Dispositivo de caractere	15:05
tty0	0 byte	Dispositivo de caractere	15:05
tty1	0 byte	Dispositivo de caractere	18:05

Dispositivos de DVD detectados: /dev/sr1

After opening the DVD, the program will analyze the DVD structure and show a preview of the disc to be ripped (next page, top left).



Fonte: FOR_A_FEW_DOLLARS_MORE, 720x480 (640x480), 4:3, 23,976 FPS, 1 Audio Track, 4 Subtitle Tracks

Título: 1 - 02h11m39s   Intervalo: Capítulos: 1 - 32

Predefinido: Official > General > Fast 1080p30

Formato: MPEG-4 (avformat)

□ Otimizado para Web
☑ Alinhar ao Início do A/V
□ Suporte ao iPod 5G
☑ Passthru Common Metadata

Duração: 02:11:39

Faixas: H.264 (x264), 30 FPS PFR
English, AAC (avcodec), Stereo
Foreign Audio Scan, Forced Only, Burned
Chapter Markers

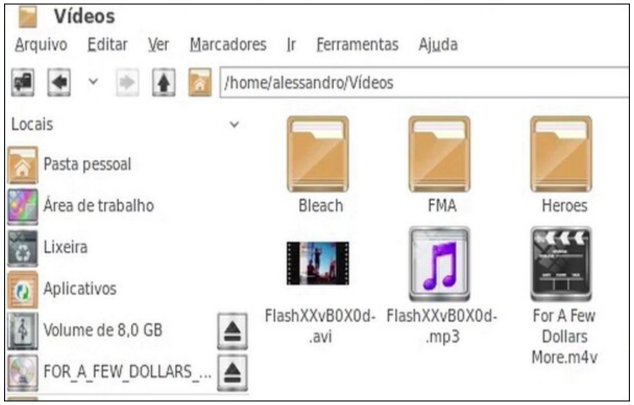
Filtros: Comb Detect, Decomb

Tamanho: 718x276 storage, 638x276 display
8:9 Pixel Aspect Ratio
2,31:1 Display Aspect Ratio

From then on, it works semi-automatically. I just chose, in the video tab, that the FPS would be the same as the source, and, in the subtitles tab, I chose to overlay the subtitles on the resulting video (each case will be different, because of the variety of existing DVDs). The audio tracks could be chosen in the audio tab, and so on.

The Video format should be set to MP4 to ensure the best web browser compatibility.

And once converted, the MP4 video file will be in the Videos folder.

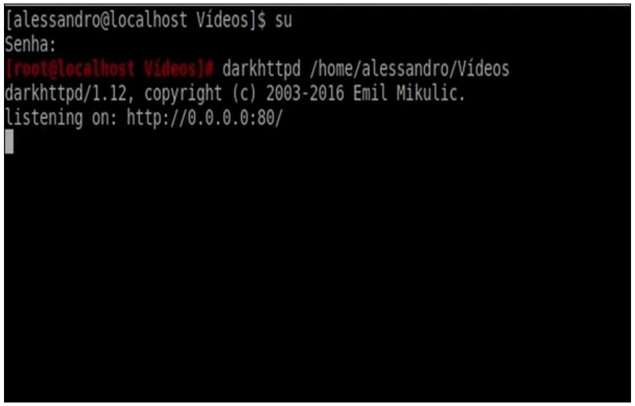


Well, the first part is done. Now let's start the Darkhttpd web server.

Second part

Now, as root, type:
  darkhttpd /home/your_user/Videos

And, the web server will start working.



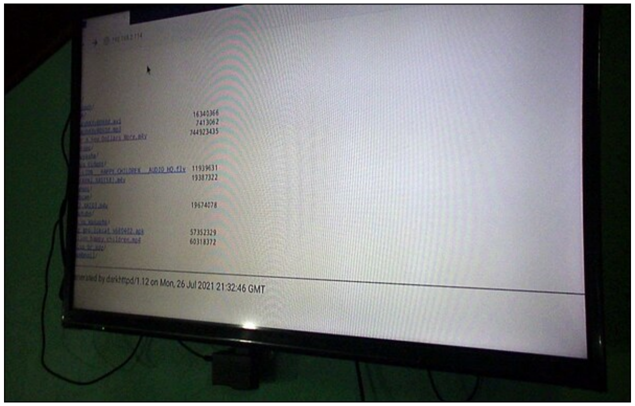
```
[alessandro@localhost Vídeos]$ su
Senha:
[root@localhost Vídeos]# darkhttpd /home/alessandro/Vídeos
darkhttpd/1.12, copyright (c) 2003-2016 Emil Mikulic.
listening on: http://0.0.0.0:80/
```

Darkhttpdworking

Now, let's go to the Smart TV, and play the converted MP4 video file.

I installed IceCat Mobile, the free derivative of Firefox, made by FSF, on this TV.

And after opening IceCat and pointing to the address of my computer running the WEB server, the screen looks like this (top, right):



And by clicking on the video file, the result is what we wanted: playing on the smart TV a video file, originating from a DVD.

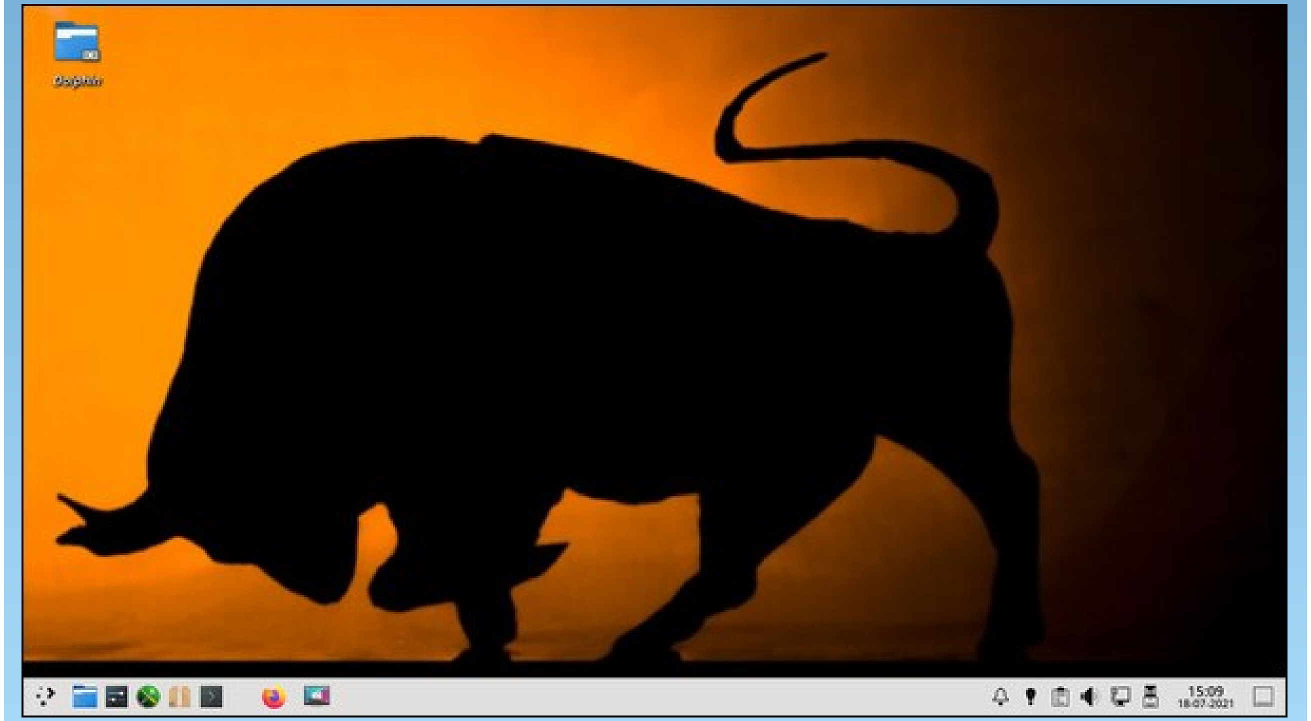
With this tip, I was able to play converted DVD files without problems, and since there is no decoding involved, since Darkhttpd only sends the file over the network, the limit will be your bandwidth, to be able to run files of higher resolutions, such as Blu Rays and even other media. I have not tested with more than one TV at the same time, but in theory, it should be possible. And, with a web server, you can even stream to cell phones, tablets, and other mobile devices.

FREE SOFTWARE FOUNDATION

I hope you enjoyed this quick tip, and that you can watch your DVD collections without problems on your smart TV's around the house.

And here, a video of the whole process.

Screenshot Showcase



Posted by mutse, July 18, 2021, running Mate.

Good Words, Good Deeds, Good News

Compiled by Meemaw

Neighbors Donate 800 Cars

In the February, 2021 issue, we reported on Chris Lewis, from North Carolina, who was restoring cars for his neighbors in need. In South Carolina, Eliot Middleton is doing the same, repairing cars for his neighbors.

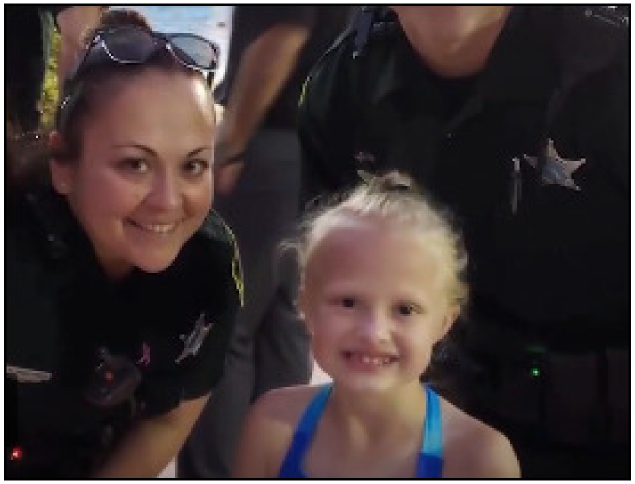
"There's no public transportation," Middleton told CBS in June. "There's no Ubers, there's no taxis or nothing like that."

His story has already made national headlines. CBS covered him in June, describing his property being full of cars and his efforts to refurbish those cars for people in need. Since then, he has had over 800 cars donated to the cause. His sister has formed the Village 2 Village Foundation in response to his effort and the massive donations which also included over $100,000 in cash.

Eight Year-Old Named Citizen of the Year

Arianna was in Florida for a cheerleading competition. She was at the hotel pool, playing when she spotted a child face down in the water. She did not know how to swim at the time and didn't know what to do during an emergency such as that one, but she took action.

"I know that whenever you see somebody you want to make sure they're okay," she explained.

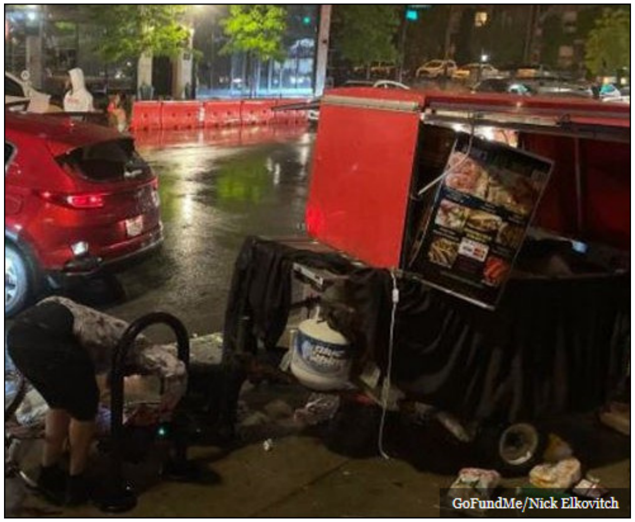


She flipped the child over, and brought her to the edge of the swimming pool, then called to adults nearby for help. The adults performed CPR and after deputies arrived, the child was revived.

In recognition of her heroism, Orange County Sheriff's Office in Orlando named her Citizen of the Year.

Community Rallies Around Business Owner

Adam Wallace is an Ohio business owner who has two food carts and a food truck. One night, the police called and told him there had been an auto accident and someone had crashed into one of his food carts and it had caught fire. The fire was put out, and Adam learned that his cook was safe.


GoFundMe/Nick Elkovitch

Nick, a service manager at a nearby cafe, started a GoFundMe page for Adam in case he wasn't insured (he is). He was very touched by their generosity.

"Just the support from the community. I appreciate you guys," said Wallace. "You have no idea how much that means to me. I know you all love my food, but that is just love on top of love."

Boy Runs in Honor of Police Officer

Twelve-year-old Zechariah Cartledge is honoring fallen Illinois officer Chris Oberheim by running one mile with a thin blue line American flag.

Zechariah founded the non-profit Running 4 Heroes, Inc., with the goal of honoring those who make the ultimate sacrifice in the line of duty. Officer Oberheim was killed in the line of duty responding to a

domestic disturbance early Wednesday morning in Champaign, Illinois. The suspect had been charged with domestic violence and possession of drugs, but during the disturbance, he was shot and killed. Oberheim's partner was shot as well, but has survived.

Zechariah ran ten laps around his elementary school track in Florida. He was joined by local Florida law enforcement officials, as well as Chief Raymond Garivey of the Freeport Police Department in Texas. He plans on giving the flag to Oberheim's family.

Paralyzed Teen Walks For Graduation

Hayden Hamilton was paralyzed from his neck down due to a spinal injury sustained in 2018 at a high school football game. However, in June, he walked across the football field to receive his high school diploma. He was assisted by his therapist, and used a brace and a walker. His graduating class broke into cheers and applause and gave him a standing ovation.

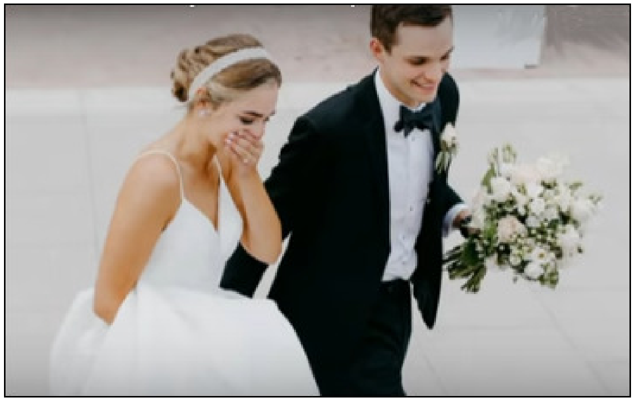
"I just wanted to be able to walk off that field again because I never got to do it that night [of the injury]. I'd say that was the main goal, to walk off that field once more," he explained.

Dog Saves Owner from Rattlesnake and Survives

Marley, the seven-year-old Labrador Retriever, heard the snake that was about to attack his owner, 18 year-old Alex Loredo. Alex had been going out to the clothes dryer which is out behind his house. Marley pushed Alex out of the way and got between him and the snake, causing the snake to strike and bite Marley twice.

Alex and his mother got Marley to the veterinarian office where they administered antivenin and admitted Marley to the animal hospital for two weeks. Marley has made an almost full recovery, still having some nerve damage on his tongue and jaw. Alex created a GoFundMe page to get help with the vet expenses.

Community Rallies to Save Couple's Wedding Day



Elizabeth and Jake Landuyt had just gotten married and were at their reception when a nearby building caught fire, forcing them to evacuate the reception area and go back to the church. They prayed for everyone's safety, and found out everyone was unhurt and the building was saved.

They wondered how they could continue their reception, but didn't know that the community had run with an idea. The venue's chef took the 120 meals that were only halfway prepared, and told his staff to take them to the restaurant next door. They finished the food and took it to a resort with space available. Whatever they lacked, another nearby restaurant provided. Neighbors volunteered for necessary jobs, one stepping up to act as bartender and one person helping carry the flowers down to the "new" venue. In less than an hour, the reception was on again.

DJ Raises Money To Fix Vehicle

A Chicago DJ driving to work saw a young man walking, on several occasions. Giving him a ride, "Ramblin Ray" Stevens found that Braxton Mayes was walking to work because his truck had broken down. He learned that Braxton had to leave home at

4:00 a.m. to get to work by 7:00 a.m., as it was a 3-hour walk each way.

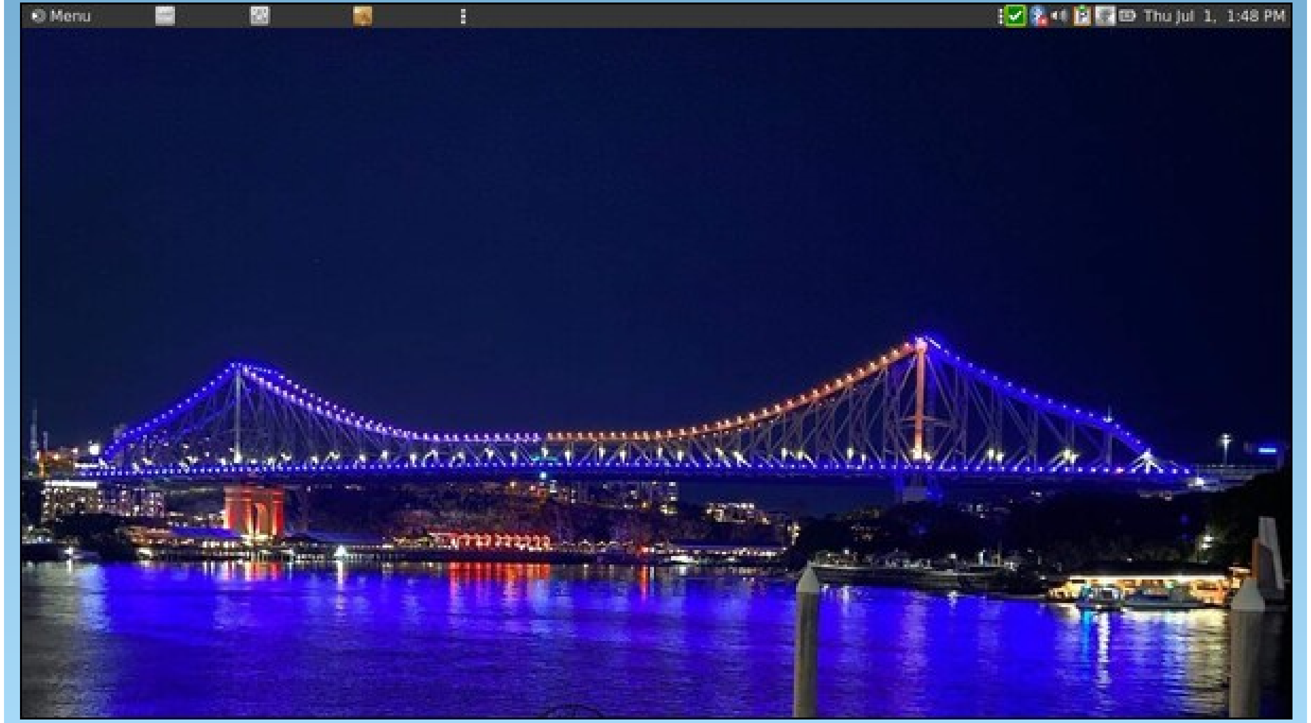
"This guy checks all the boxes," Stevens noted. "He's a good, solid human being. People are having a hard time finding people to work and here's a guy walking three hours one way just because his truck broke down."

Stevens created a GoFundMe page which has raised more than its $10,000 goal. Stevens posted, *"Let's help Braxton get his truck fixed! Any other left over money will go to Chicago area food banks."*

Mayes said *"It brought me to tears. I didn't know when I would come up with the money to fix it or how many times I would have to walk."* His employer is giving him a ride right now, but his truck should be fixed soon.

30TH
ANNIVERSARY
OF LINUX
1991-2021
#30YearsofLinux
100% of the world's top 500 supercomputers **run on Linux.** Not bad for 30.
THE LINUX FOUNDATION

Screenshot Showcase



Posted by brisvegas, July 1, 2021, running Mate.

Email Self Defense: A Guide To Fighting Surveillance With GnuPG Encryption

Reprinted from the **Free Software Foundation**
Images used via Creative Commons Attribution 4.0 license
Text used via Creative Commons Attribution-ShareAlike 4.0 license

Bulk surveillance violates our fundamental rights and makes free speech risky. This guide will teach you a basic surveillance self-defense skill: email encryption. Once you've finished, you'll be able to send and receive emails that are scrambled to make sure a surveillance agent or thief intercepting your email can't read them. All you need is a computer with an Internet connection, an email account, and about forty minutes.

Even if you have nothing to hide, using encryption helps protect the privacy of people you communicate with, and makes life difficult for bulk surveillance systems. If you do have something important to hide, you're in good company; these are the same tools that whistleblowers use to protect their identities while shining light on human rights abuses, corruption, and other crimes.

In addition to using encryption, standing up to surveillance requires fighting politically for a reduction in the amount of data collected on us, but the essential first step is to protect yourself and make surveillance of your communication as difficult as possible. This guide helps you do that. It is designed for beginners, but if you already know the basics of GnuPG or are an experienced free software user, you'll enjoy the advanced tips and the guide to teaching your friends.

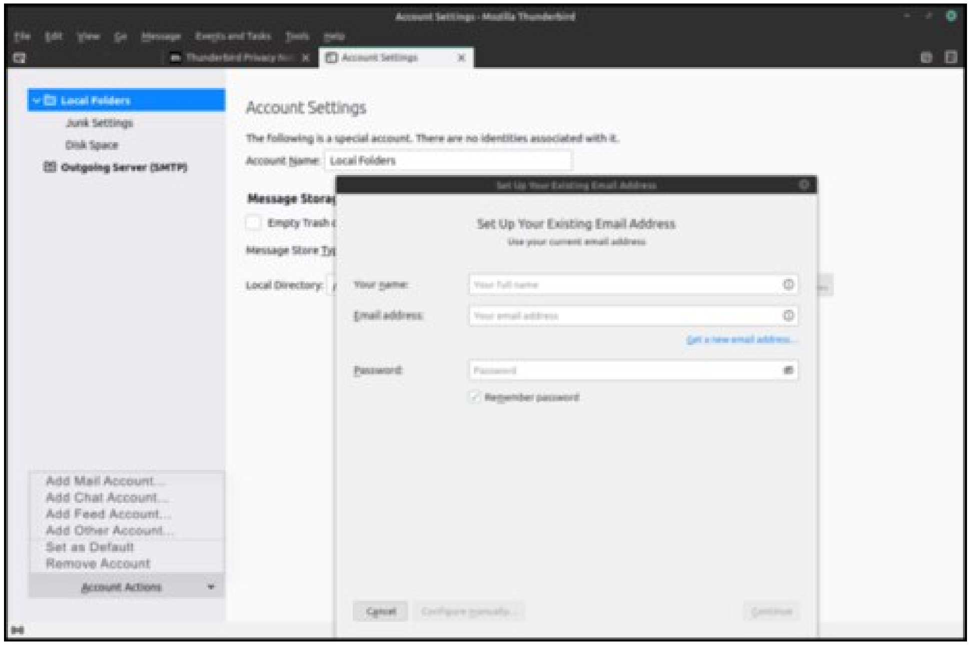
Section #1: Get The Pieces

This guide relies on software which is freely licensed; it's completely transparent and anyone can copy it or make their own version. This makes it safer from surveillance than proprietary software (like Windows or macOS). Learn more about free software at fsf.org.

Most GNU/Linux operating systems come with GnuPG installed on them, so if you're running one of these systems, you don't have to download it. If you're running macOS or Windows, steps to download GnuPG are below. Before configuring your encryption setup with this guide, though, you'll need a desktop email program installed on your computer. Many GNU/Linux distributions have one installed already, such as Icedove, which may be under the alternate name "Thunderbird." Programs like these are another way to access the same email accounts you can access in a browser (like Gmail), but provide extra features.

If you already have an email program, you can skip to Step 2.

Step #1.a: Set Up Your Email Program With Your Email Account



Open your email program and follow the wizard (step-by-step walkthrough) that sets it up with your email account. This usually starts from "Account Settings" → "Add Mail Account". You should get the email server settings from your systems administrator or the help section of your email account.

Troubleshooting

The wizard doesn't launch. You can launch the wizard yourself, but the menu option for doing so is named differently in each email program. The button to launch it will be in the program's main menu, under "New" or something similar, titled something like "Add account" or "New/Existing email account."

The wizard can't find my account or isn't downloading my mail. Before searching the Web, we recommend you start by asking other people who use your email system, to figure out the correct settings.

I can't find the menu. In many new email programs, the main menu is represented by an image of three stacked horizontal bars.

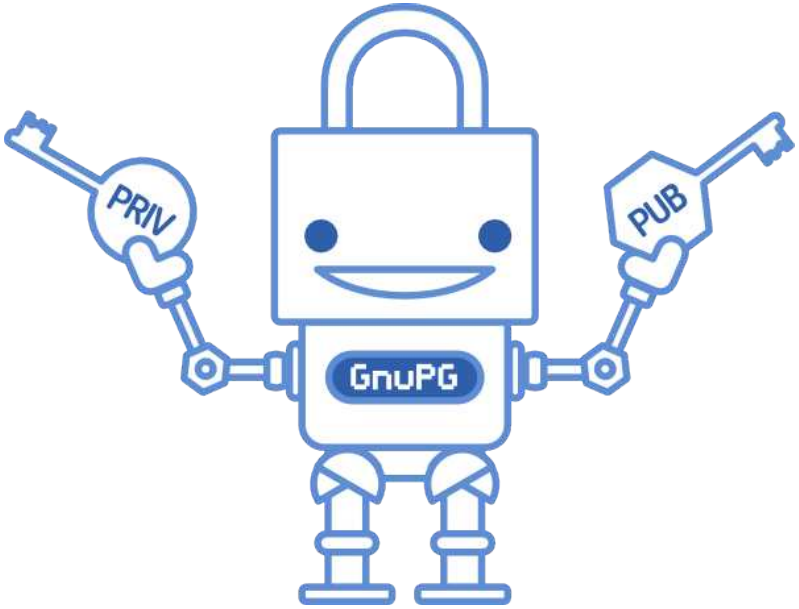
Step #1.b: Get Your Terminal Ready And Install Gnupg

If you are using a GNU/Linux machine, you should already have GnuPG installed, and you can skip to Step 2.

GnuPG, OpenPGP, what?

In general, the terms GnuPG, GPG, GNU Privacy Guard, OpenPGP and PGP are used interchangeably. Technically, OpenPGP (Pretty Good Privacy) is the encryption standard, and GNU Privacy Guard (often shortened to GPG or GnuPG) is the program that implements the standard. Most email programs provide an interface for GnuPG. There is also a newer version of GnuPG, called GnuPG2.

Section #2: Make Your Keys



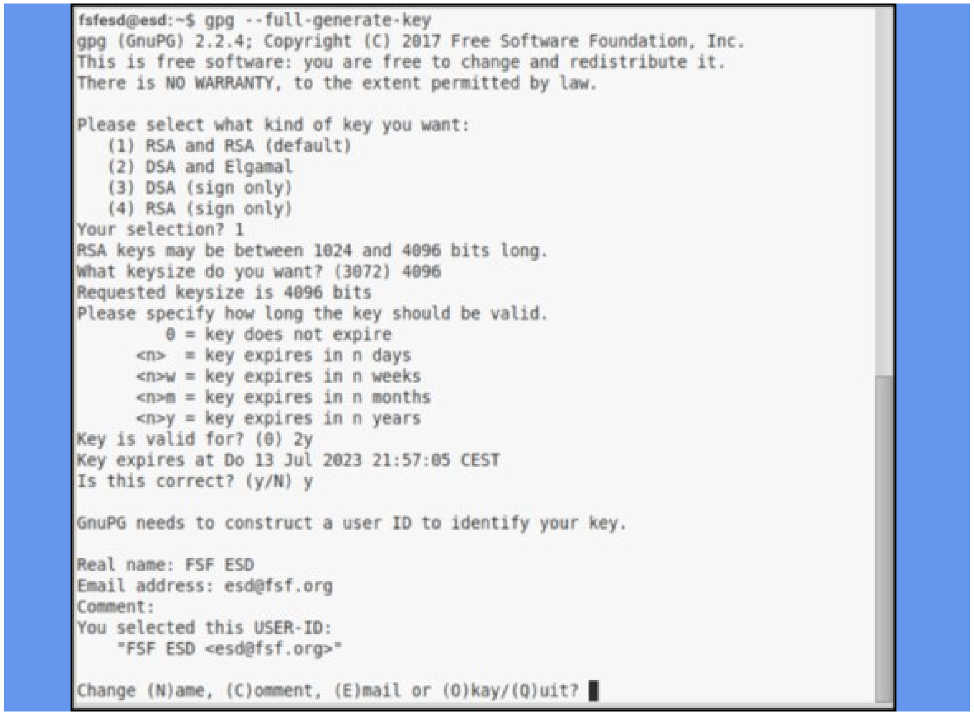
To use the GnuPG system, you'll need a public key and a private key (known together as a keypair). Each is a long string of randomly generated numbers and letters that are unique to you. Your public and private keys are linked together by a special mathematical function.

Your public key isn't like a physical key, because it's stored in the open in an online directory called a keyserver. People download it and use it, along with GnuPG, to encrypt emails they send to you. You can think of the keyserver as a phonebook; people who want to send you encrypted email can look up your public key.

Your private key is more like a physical key, because you keep it to yourself (on your computer). You use GnuPG and your private key together to descramble encrypted emails other people send to you. **You should never share your private key with anyone, under any circumstances.**

In addition to encryption and decryption, you can also use these keys to sign messages and check the authenticity of other people's signatures. We'll discuss this more in the next section.

Step #2.a: Make A Keypair



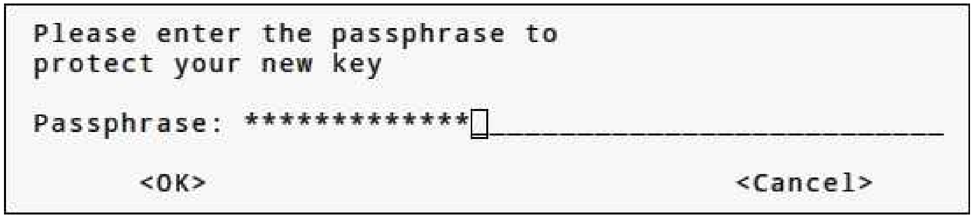
```
fsfesd@esd:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 2y
Key expires at Do 13 Jul 2023 21:57:05 CEST
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: FSF ESD
Email address: esd@fsf.org
Comment:
You selected this USER-ID:
    "FSF ESD <esd@fsf.org>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```



```
Please enter the passphrase to
protect your new key

Passphrase: *************_____________________________

      <OK>                                   <Cancel>
```

Open a terminal using **`ctrl + alt + t`** (on GNU/linux), or find it in your applications, and use the following code to create your keypair:

We will use the command line in a terminal to create a keypair using the GnuPG program. A terminal should be installed on your GNU/Linux operating system, if you are using a macOS or Windows OS system, use the programs "Terminal" (macOS) or "PowerShell" (Windows) that were also used in section 1.

`# gpg --full-generate-key` to start the process.

# To answer what kind of key you would like to create, select the default option **`1 RSA and RSA`**.

# Enter the following keysize: **`4096`** for a strong key.

# Choose the expiration date, we suggest **`2y`** (2 years).

Follow the prompts to continue setting up with your personal details.

Set Your Passphrase

On the screen titled "Passphrase," pick a strong password! You can do it manually, or you can use the Diceware method. Doing it manually is faster but not as secure. Using Diceware takes longer and requires dice, but creates a password that is much harder for attackers to figure out. To use it, read the section "Make a secure passphrase with Diceware" in this article by Micah Lee.

If you'd like to pick a passphrase manually, come up with something you can remember which is at least twelve characters long, and includes at least one lower case and upper case letter and at least one number or punctuation symbol. Never pick a password you've used elsewhere. Don't use any recognizable patterns, such as birthdays, telephone numbers, pets' names, song lyrics, quotes from books, and so on.

Troubleshooting

GnuPG is not installed. GPG is not installed. You can check if this is the case with the command **`gpg --version`**. If GnuPG is not installed, it would bring up the following result on most GNU/Linux operating systems, or something like it: **`Command 'gpg' not found, but can be installed with: su- apt-get install gnupg.`** Follow that command and install the program.

I took too long to create my passphrase. That's okay. It's important to think about your passphrase. When you're ready, just follow the steps from the beginning again to create your key.

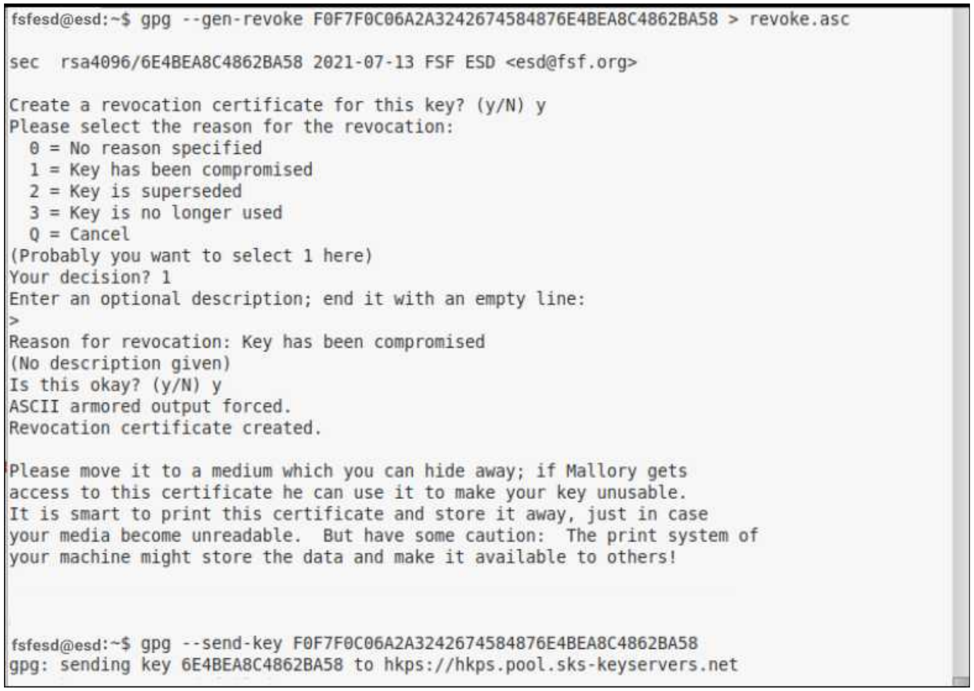
How can I see my key? Use the following command to see all keys **`gpg --list-keys`**. Yours should be listed in there, and later, so will Edward's (section 3). If you want to see only your key, you can use **`gpg --list-key [your@email]`**. You can also use **`gpg --list-secret-key`** to see your own private key.

More resources. For more information about this process, you can also refer to The GNU Privacy Handbook. Make sure you stick with "RSA and RSA" (the default), because it's newer and more secure than the algorithms the documentation recommends. Also make sure your key is at least 4096 bits if you want to be secure.

Advanced

Advanced key pairs. When GnuPG creates a new keypair, it compartmentalizes the encryption function from the signing function through subkeys. If you use subkeys carefully, you can keep your GnuPG identity more secure and recover from a compromised key much more quickly. Alex Cabal and the Debian wiki provide good guides for setting up a secure subkey configuration.

Step #2.b: Some Important Steps Following Creation



```
fsfesd@esd:~$ gpg --gen-revoke F0F7F0C06A2A3242674584876E4BEA8C4862BA58 > revoke.asc

sec  rsa4096/6E4BEA8C4862BA58 2021-07-13 FSF ESD <esd@fsf.org>

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? 1
Enter an optional description; end it with an empty line:
>
Reason for revocation: Key has been compromised
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!



fsfesd@esd:~$ gpg --send-key F0F7F0C06A2A3242674584876E4BEA8C4862BA58
gpg: sending key 6E4BEA8C4862BA58 to hkps://hkps.pool.sks-keyservers.net
```

We will upload your key to a keyserver, so if someone wants to send you an encrypted message, they can download your public key from the Internet. There are multiple keyservers that you can select from the menu when you upload, but they are all copies of each other, so it doesn't matter which one you use. However, it sometimes takes a few hours for them to match each other when a new key is uploaded.

# Copy your keyID **`gnupg --list-key [your@email]`** will list your public ("pub") key information, including your keyID, which is a unique list of numbers and letters. Copy this keyID, so you can use it in the following command.

# Upload your key to a server: **`gpg --send-key [keyID]`**

Export Your Key To A File

Use the following command to export your secret key so you can import it into your email client at the next step. To avoid getting your key compromised, store this in a safe place, and make sure that if it is transferred, it is done so in a trusted way. Exporting your keys can be done with the following commands:

```
$ gpg --export-secret-keys -a [keyid] > my_secret_key.asc
$ gpg --export -a [keyid] > my_public_key.asc
```

Generate A Revocation Certificate

Just in case you lose your key, or it gets compromised, you want to generate a certificate and choose to save it in a safe place on your computer for now (please refer to step 6.C for how to best store your revocation certificate safely). This step is essential for your email self-defense, as you'll learn more about in Section 5.

# Copy your keyID **`gnupg --list-key [your@email]`** will list your public ("pub") key information, including your keyID, which is a unique list of numbers and letters. Copy this keyID, so you can use it in the following command.

# Generate a revocation certificate: **`gpg --gen-revoke --output revoke.asc [keyID]`**

# It will prompt you to give a reason for revocation, we recommend to use **`1 "key has been compromised"`**

# You don't have to fill in a reason, but you can, then press enter for an empty line, and confirm your selection.

Troubleshooting

My key doesn't seem to be working or I get a "permission denied." Like every other file or folder, gpg keys are subject to permissions. If these are not set correctly, your system may not be accepting your keys. You can follow the next steps to check, and update to the right permissions.

# Check your permissions: **`ls -l ~/.gnupg/*`**

# Set permissions to read, write, execute for only yourself, no others. This is the recommended permission for your folder. You can use the code: **`chmod 700 ~/.gnupg`**.

# Set permissions to read and write for yourself only, no others. This is the recommended permission for the keys inside your folder. You can use the code: **`chmod 600 ~/.gnupg/*`**.

If you have (for any reason) created your own folders inside ~/.gnupg, you must also additionally apply execute permissions to that folder. Folders require execution privileges to be opened. For more information on permissions, you can check out this detailed information guide.

Advanced

More about keyservers. You can find some more keyserver information in this manual. The sks Web site maintains a list of highly interconnected keyservers. You can also directly export your key as a file on your computer.

Transferring your keys. Use the following commands to transfer your keys. To avoid getting your key compromised, store it in a safe place, and make sure that if it is transferred, it is done so in a trusted way. Importing and exporting a key can be done with the following commands:

```
$ gpg --export-secret-keys -a keyid > my_private_key.asc
$ gpg --export -a keyid > my_public_key.asc
$ gpg --import my_private_key.asc
$ gpg --import my_public_key.asc
```

Ensure that the keyID printed is the correct one, and if so, then go ahead and add **ultimate** trust for it:

```
$ gpg --edit-key [your@email]
```

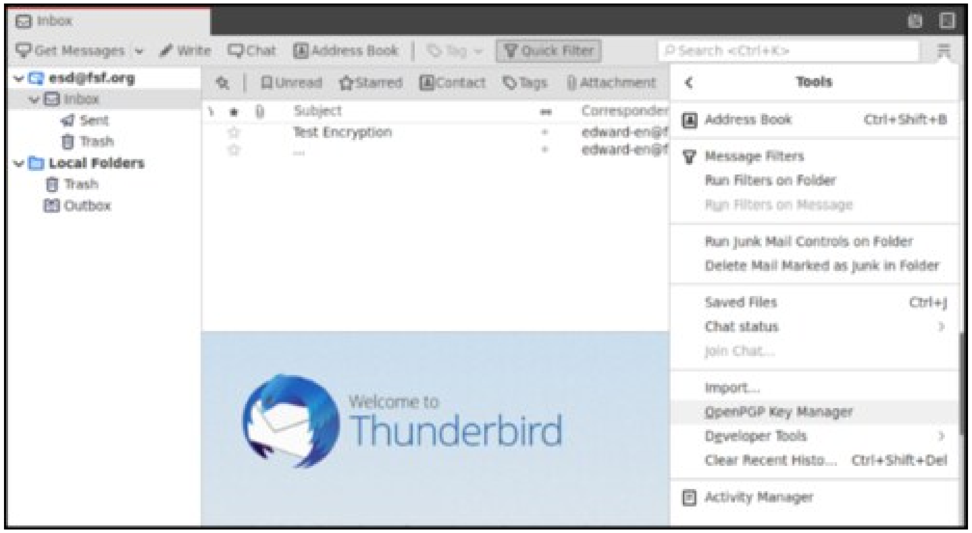
Because this is your key, you should choose ultimate. You shouldn't trust anyone else's key ultimately.

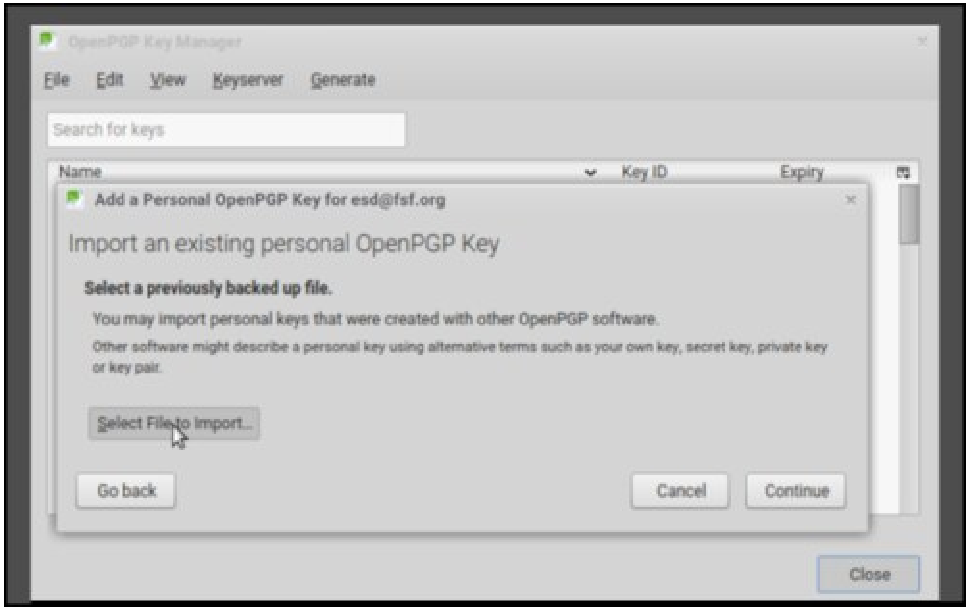
Refer to troubleshooting in step 2.B for more information on permissions. When transferring keys, your permissions may get mixed, and errors may be prompted. These are easily avoided when your folders and files have the right permissions

Section #3: Set Up Email Encryption

The Icedove (or Thunderbird) email program has PGP functionality integrated, which makes it pretty easy to work with. We'll take you through the steps of integrating and using your key in these email clients.

Step #3.a: Set Up Your Email With Encryption



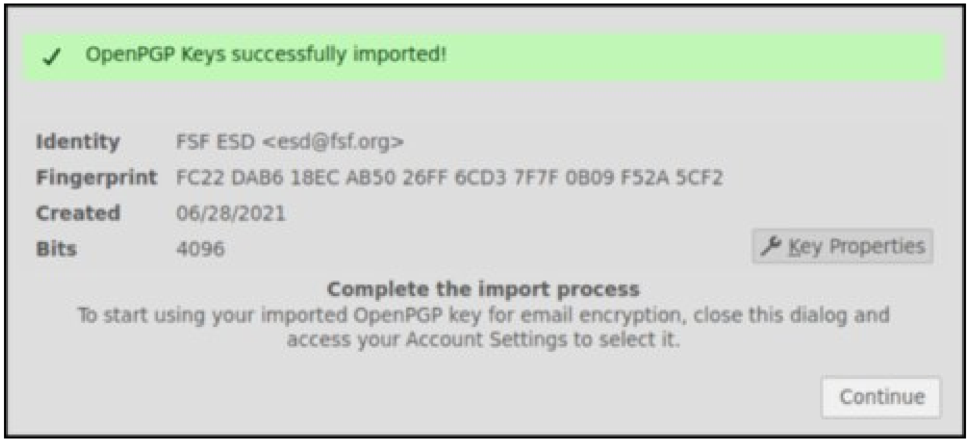


Import an existing personal OpenPGP Key

Select a previously backed up file.

You may import personal keys that were created with other OpenPGP software.

Other software might describe a personal key using alternative terms such as your own key, secret key, private key or key pair.



✓ OpenPGP Keys successfully imported!

Identity FSF ESD <esd@fsf.org>
Fingerprint FC22 DAB6 18EC AB50 26FF 6CD3 7F7F 0B09 F52A 5CF2
Created 06/28/2021
Bits 4096

Complete the import process
To start using your imported OpenPGP key for email encryption, close this dialog and access your Account Settings to select it.

Once you have set up your email with encryption, you can start contributing to encrypted traffic on the Internet. First we'll get your email client to import your secret key, and we will also learn how to get other people's public keys from servers so you can send and receive encrypted email.

# Open your email client and use "Tools" → **OpenPGP Manager**.

# Under "File" → **Import Secret Key(s) From File**.

# Select the file you saved under the name [my_secret_key.asc] in step step 3.b when you exported your key.

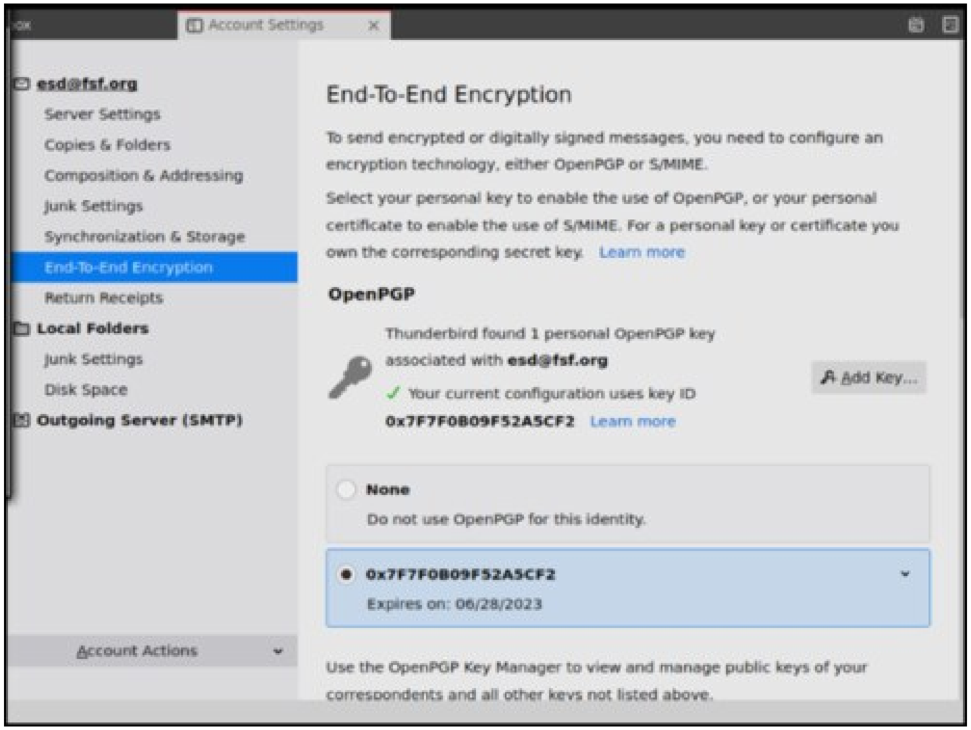
# Unlock with your passphrase.

# You will receive a "OpenPGP keys successfully imported" window to confirm success.

# Go to "Edit" (in Icedove) or "Tools" (in Thunderbird) → "Account settings" → "End-To-End Encryption," and make sure your key is imported and select Treat this key as a Personal Key.

Troubleshooting

I'm not sure the import worked correctly. Look for "Account settings" → "End-To-End Encryption" (Under "Edit" (in Icedove) or "Tools" (in Thunderbird)). Here you can see if your personal key associated with this email is found. If it is not, you can try again via the **Add key** option. Make sure you have the correct, active, secret key file.



End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more

OpenPGP

Thunderbird found 1 personal OpenPGP key associated with esd@fsf.org

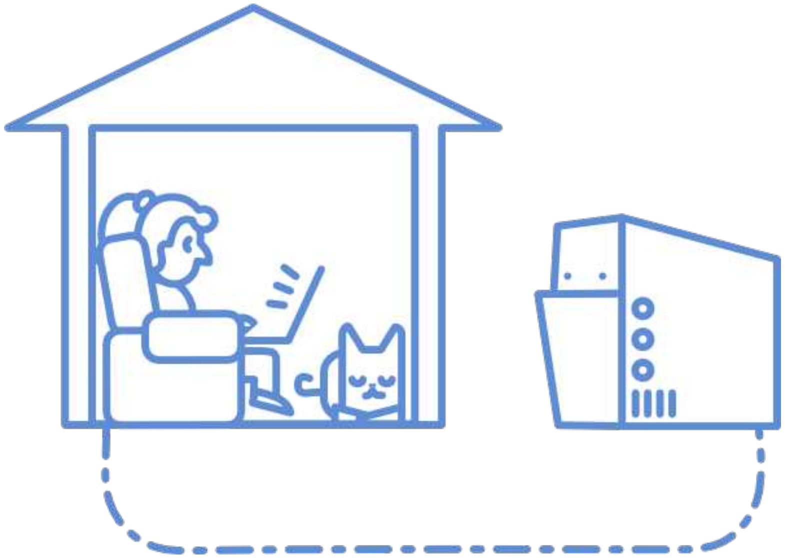
✓ Your current configuration uses key ID 0x7F7F0B09F52A5CF2 Learn more

○ None
Do not use OpenPGP for this identity.

● 0x7F7F0B09F52A5CF2
Expires on: 06/28/2023

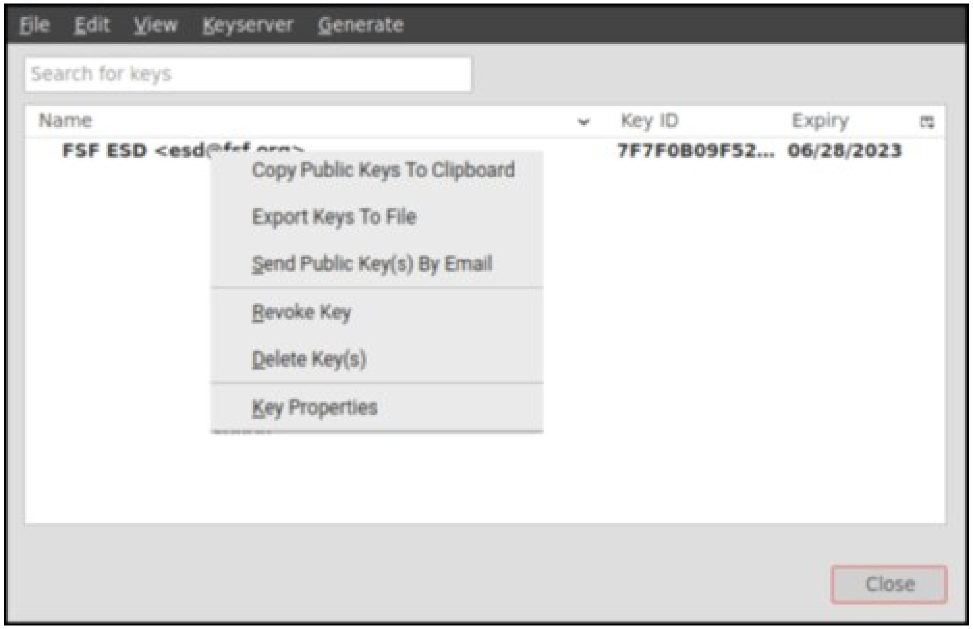
Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

Section #4: Try It Out!



Now you'll try a test correspondence with an FSF computer program named Edward, who knows how to use encryption. Except where noted, these are the same steps you'd follow when corresponding with a real, live person.

Step #4.a: Send Edward Your Public Key



Name	Key ID	Expiry
FSF ESD <esd@fsf.org>	7F7F0B09F52...	06/28/2023

This is a special step that you won't have to do when corresponding with real people. In your email program's menu, go to "Tools" → "OpenPGP Key Manager." You should see your key in the list that pops up. Right click on your key and select **Send Public Keys by Email**. This will create a new draft message, as if you had just hit the "Write" button, but in the attachment you will find your public keyfile.

Address the message to **edward-en@fsf.org**. Put at least one word (whatever you want) in the subject and body of the email. Don't send yet.

We want Edward to be able to open the email with your keyfile, so we want this first special message to be unencrypted. Make sure encryption is turned off by using the dropdown menu "Security" and select **Do Not Encrypt**. Once encryption is off, hit Send.

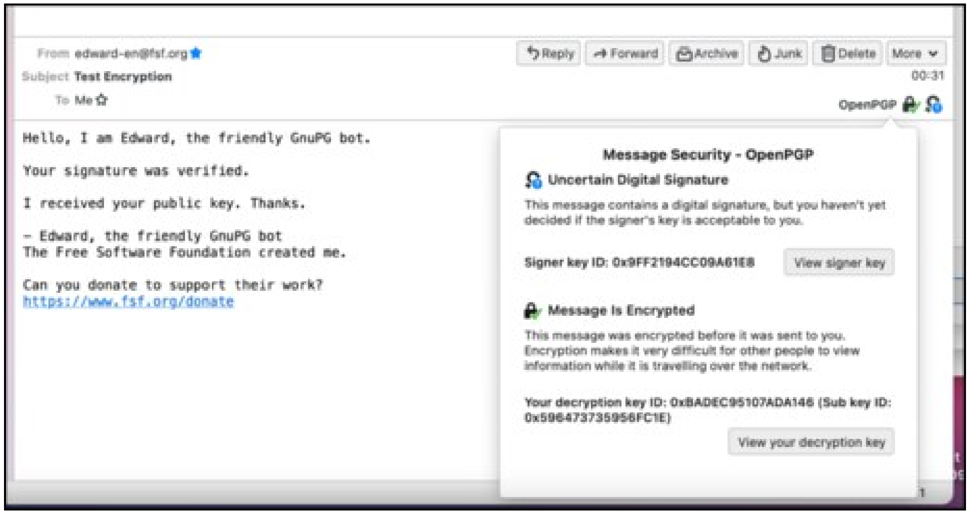
It may take two or three minutes for Edward to respond. In the meantime, you might want to skip ahead and check out the **Use it Well** section of this guide. Once you have received a response, head to the next step. From here on, you'll be doing just the same thing as when corresponding with a real person.

When you open Edward's reply, GnuPG may prompt you for your passphrase before using your private key to decrypt it.

Step #4.b: Send A Test Encrypted Email

Get Edward's key

To encrypt an email to Edward, you need its public key, so now you'll have to download it from a keyserver. You can do this in two different ways:



From edward-en@fsf.org
Subject Test Encryption
00:31
To Me

```
Hello, I am Edward, the friendly GnuPG bot.

Your signature was verified.

I received your public key. Thanks.

- Edward, the friendly GnuPG bot
The Free Software Foundation created me.

Can you donate to support their work?
https://www.fsf.org/donate
```

Message Security - OpenPGP

Uncertain Digital Signature

This message contains a digital signature, but you haven't yet decided if the signer's key is acceptable to you.

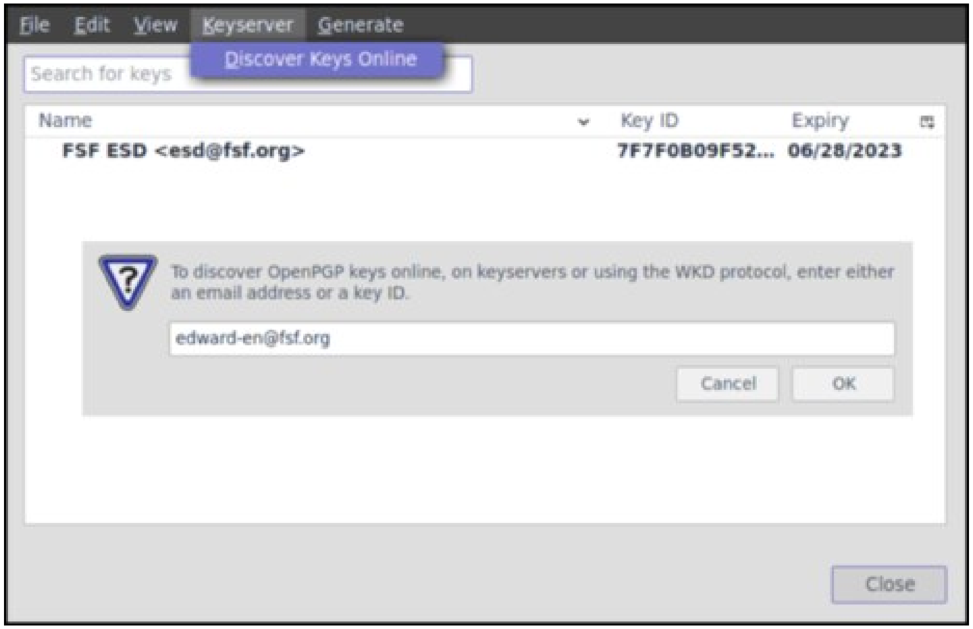
Signer key ID: 0x9FF2194CC09A61E8

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is travelling over the network.

Your decryption key ID: 0xBADEC95107ADA146 (Sub key ID: 0x596473735956FC1E)

Option 1. In the email answer you received from Edward as a response to your first email, Edward's public key was included. On the right of the email, just above the writing area, you will find an "OpenPGP" button that has a lock and a little wheel next to it. Click that, and select **Discover** next to the text: "This message was sent with a key that you don't have yet." A popup with Edward's key details will follow.



Name	Key ID	Expiry
FSF ESD <esd@fsf.org>	7F7F0B09F52...	06/28/2023

To discover OpenPGP keys online, on keyservers or using the WKD protocol, enter either an email address or a key ID.

edward-en@fsf.org

Option 2. Open your OpenPGP manager and under "Keyserver" choose Discover Keys Online. Here, fill in Edward's email address, and import Edward's key.

The option **Accepted (unverified)** will add this key to your key manager, and now it can be used to send encrypted emails and to verify digital signatures from Edward.

In the popup window confirming if you want to import Edward's key, you'll see many different emails that are all associated with its key. This is correct; you can safely import the key.

Since you encrypted this email with Edward's public key, Edward's private key is required to decrypt it. Edward is the only one with its private key, so no one except Edward can decrypt it.

Send Edward An Encrypted Email

Write a new email in your email program, addressed to **edward-en@fsf.org**. Make the subject "Encryption test" or something similar and write something in the body.

This time, make sure encryption is turned on by using the dropdown menu "Security" and select **Require Encryption**. Once encryption is on, hit Send.

Troubleshooting

"Recipients not valid, not trusted or not found". You may be trying to send an encrypted email to someone when you do not have their public key yet. Make sure you follow the steps above to import the key to your key manager. Open OpenPGP Key Manager to make sure the recipient is listed there.

Unable to send message. You could get the following message when trying to send your encrypted email: "Unable to send this message with end-to-end encryption, because there are problems with the keys of the following recipients: edward-en@fsf.org." This usually means you imported the key with the "unaccepted (unverified) option." Go to the "key properties" of this key by right clicking on the key in the OpenPGP Key Manager, and select the option **Yes, but I have not verified that this is the correct key** in the "Acceptance" option at the bottom of this window. Resend the email.

I can't find Edward's key. Close the pop-ups that have appeared since you clicked Send. Make sure you are connected to the Internet and try again. If that doesn't work, repeat the process, choosing a different keyserver when it asks you to pick one.

Unscrambled messages in the Sent folder. Even though you can't decrypt messages encrypted to someone else's key, your email program will automatically save a copy encrypted to your public key, which you'll be able to view from the Sent folder like a normal email. This is normal, and it doesn't mean that your email was not sent encrypted.

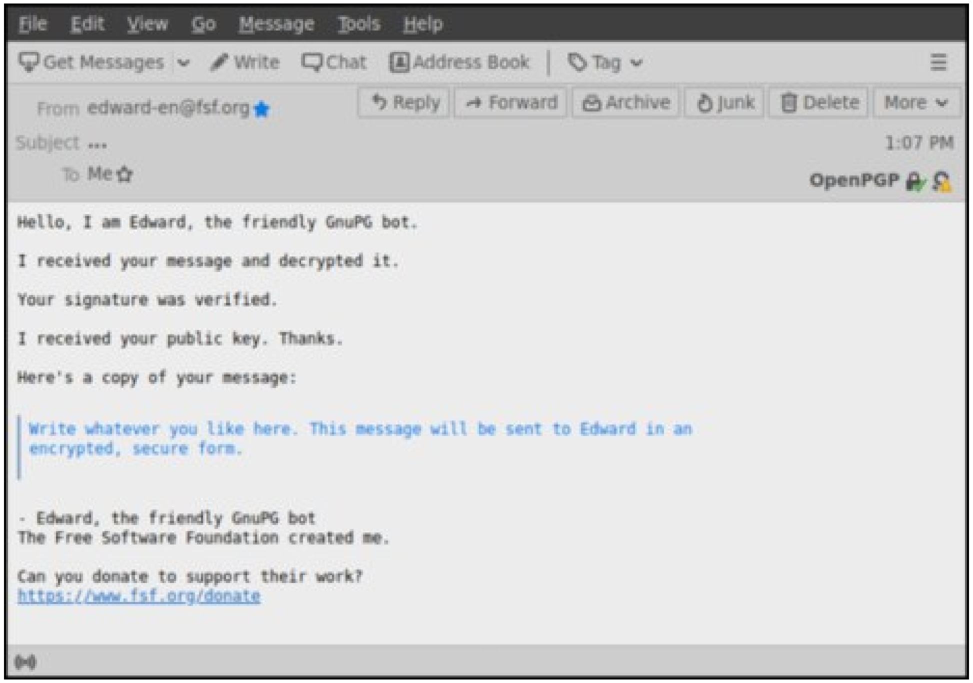
Advanced

Encrypt messages from the command line. You can also encrypt and decrypt messages and files from the command line, if that's your preference. The option --armor makes the encrypted output appear in the regular character set.

Important: Security Tips

Even if you encrypt your email, the subject line is not encrypted, so don't put private information there. The sending and receiving addresses aren't encrypted either, so a surveillance system can still figure out who you're communicating with. Also, surveillance agents will know that you're using GnuPG, even if they can't figure out what you're saying. When you send attachments, you can choose to encrypt them or not, independent of the actual email.

For greater security against potential attacks, you can turn off HTML. Instead, you can render the message body as plain text. In order to do this in Icedove or Thunderbird, go to View > Message Body As > Plain Text.



```
Hello, I am Edward, the friendly GnuPG bot.

I received your message and decrypted it.

Your signature was verified.

I received your public key. Thanks.

Here's a copy of your message:

| Write whatever you like here. This message will be sent to Edward in an
| encrypted, secure form.


- Edward, the friendly GnuPG bot
The Free Software Foundation created me.

Can you donate to support their work?
https://www.fsf.org/donate
```

Step #4.c: Receive A Response

When Edward receives your email, it will use its private key to decrypt it, then reply to you.

It may take two or three minutes for Edward to respond. In the meantime, you might want to skip ahead and check out the **Use it Well** section of this guide.

Edward will send you an encrypted email back saying your email was received and decrypted. Your email client will automatically decrypt Edward's message.

The OpenPGP button in the email will show a little green checkmark over the lock symbol to show the message is encrypted, and a little orange warning sign which means that you have accepted the key, but not verified it. When you have not yet accepted the key, you will see a little question mark there. Clicking the prompts in this button will lead you to key properties as well.

Step #4.d: Send A Signed Test Email

GnuPG includes a way for you to sign messages and files, verifying that they came from you and that they weren't tampered with along the way. These signatures are stronger than their pen-and-paper cousins -- they're impossible to forge, because they're impossible to create without your private key (another reason to keep your private key safe).

You can sign messages to anyone, so it's a great way to make people aware that you use GnuPG and that they can communicate with you securely. If they don't have GnuPG, they will be able to read your message and see your signature. If they do have GnuPG, they'll also be able to verify that your signature is authentic.

To sign an email to Edward, compose any message to the email address and click the pencil icon next to the lock icon so that it turns gold. If you sign a message, GnuPG may ask you for your password before it sends the message, because it needs to unlock your private key for signing.

In "Account Settings" → "End-To-End-Encryption" you can opt to add a digital signature by default.

Step #4.e: Receive a response

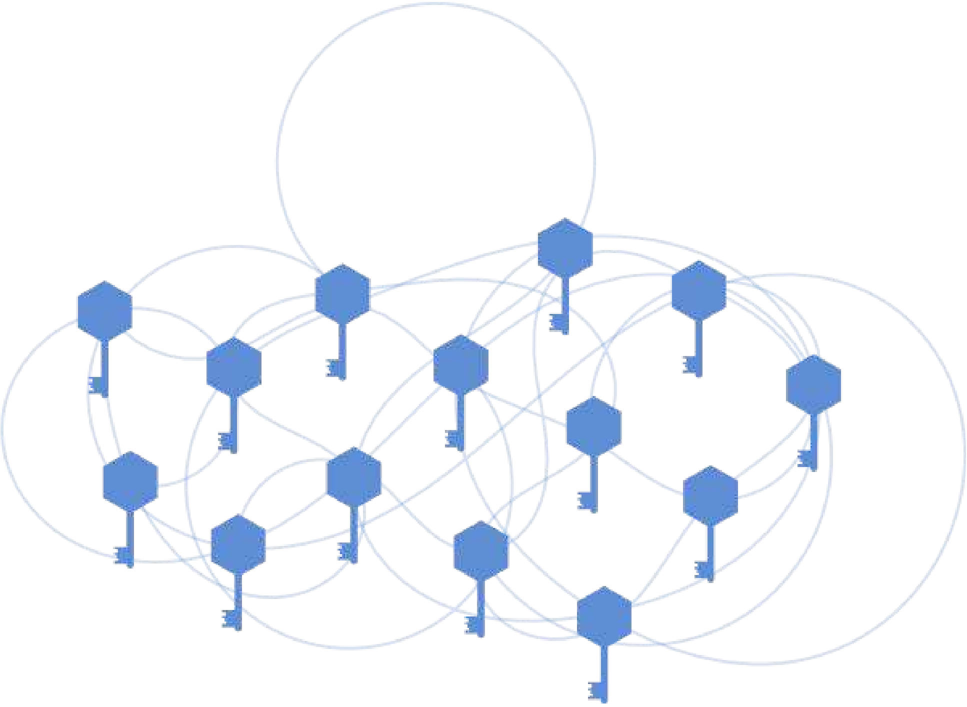
When Edward receives your email, he will use your public key (which you sent him in Step 3.a) to verify the message you sent has not been tampered with and to encrypt a reply to you.

It may take two or three minutes for Edward to respond. In the meantime, you might want to skip ahead and check out the **Use it Well** section of this guide.

Edward's reply will arrive encrypted, because he prefers to use encryption whenever possible. If everything goes according to plan, it should say "Your signature was verified." If your test signed email was also encrypted, he will mention that first.

When you receive Edward's email and open it, your email client will automatically detect that it is encrypted with your public key, and then it will use your private key to decrypt it.

Section #5: Learn About The Web Of Trust



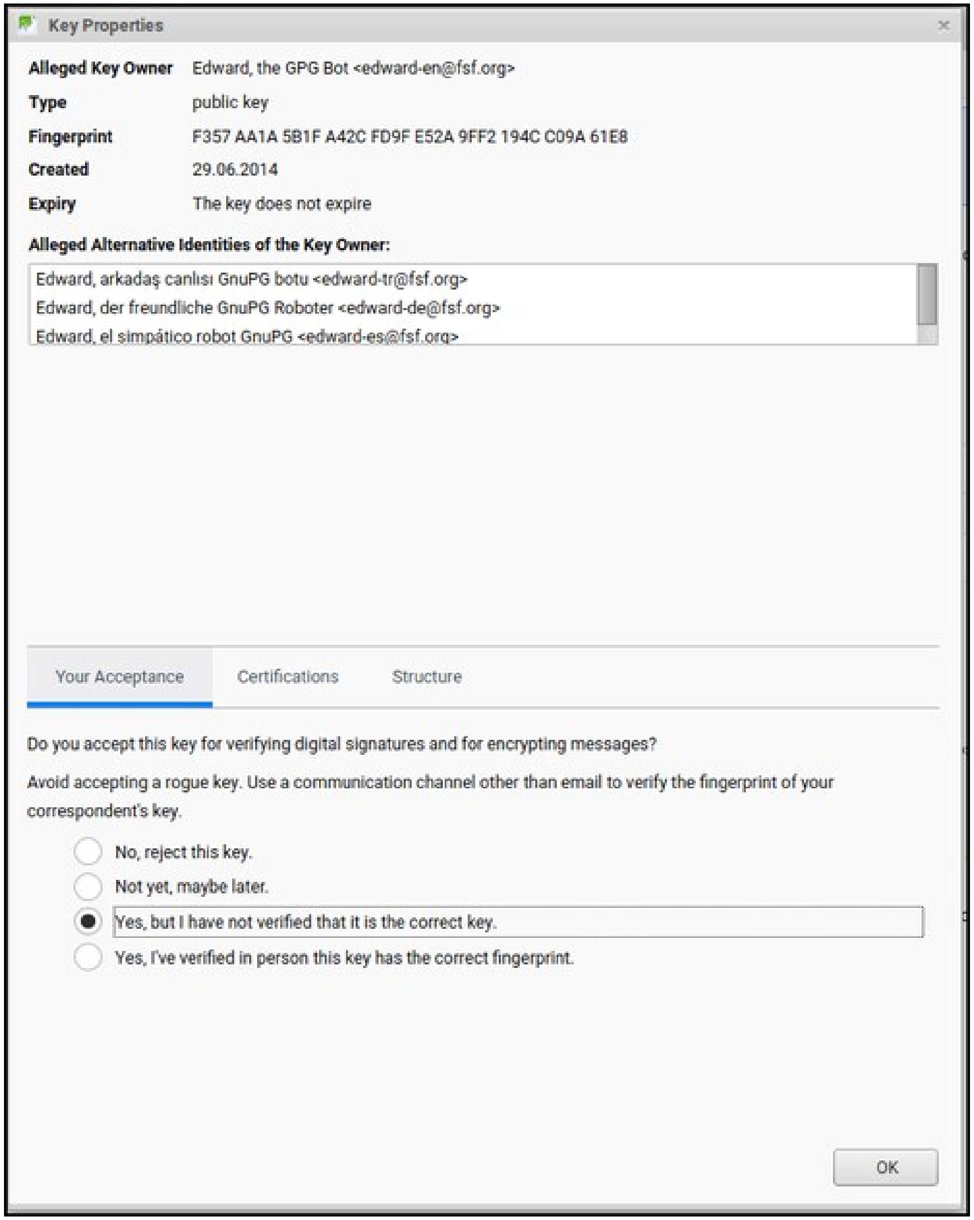
Email encryption is a powerful technology, but it has a weakness: it requires a way to verify that a person's public key is actually theirs. Otherwise, there would be no way to stop an attacker from making an email address with your friend's name, creating keys to go with it, and impersonating your friend. That's why the free software programmers that developed email encryption created keysigning and the Web of Trust.

When you sign someone's key, you are publicly saying that you've verified that it belongs to them and not someone else.

Signing keys and signing messages use the same type of mathematical operation, but they carry very different implications. It's a good practice to generally sign your email, but if you casually sign people's keys, you may accidentally end up vouching for the identity of an imposter.

People who use your public key can see who has signed it. Once you've used GnuPG for a long time, your key may have hundreds of signatures. You can consider a key to be more trustworthy if it has many signatures from people that you trust. The Web of Trust is a constellation of GnuPG users, connected to each other by chains of trust expressed through signatures.

Step #5.A: Sign A Key



Alleged Key Owner	Edward, the GPG Bot <edward-en@fsf.org>
Type	public key
Fingerprint	F357 AA1A 5B1F A42C FD9F E52A 9FF2 194C C09A 61E8
Created	29.06.2014
Expiry	The key does not expire

Alleged Alternative Identities of the Key Owner:

Edward, arkadaş canlısı GnuPG botu <edward-tr@fsf.org>
Edward, der freundliche GnuPG Roboter <edward-de@fsf.org>
Edward, el simpático robot GnuPG <edward-es@fsf.org>

Do you accept this key for verifying digital signatures and for encrypting messages?

Avoid accepting a rogue key. Use a communication channel other than email to verify the fingerprint of your correspondent's key.

○ No, reject this key.
○ Not yet, maybe later.
● Yes, but I have not verified that it is the correct key.
○ Yes, I've verified in person this key has the correct fingerprint.

In your email program's menu, go to OpenPGP Key Manager and select **Key properties** by right clicking on Edward's key.

Under "Your Acceptance," you can select **“Yes, I've verified in person this key has the correct fingerprint”**.

You've just effectively said "I trust that Edward's public key actually belongs to Edward." This doesn't mean much because Edward isn't a real person, but it's good practice, and for real people it is important. You can read more about signing a person's key in the check IDs before signing section.

Identifying Keys: Fingerprints And Ids

People's public keys are usually identified by their key fingerprint, which is a string of digits like F357AA1A5B1FA42CFD9FE52A9FF2194CC09A61E8 (for Edward's key). You can see the fingerprint for your public key, and other public keys saved on your computer, by going to OpenPGP Key Management in your email program's menu, then right clicking on the key and choosing Key Properties. It's good practice to share your fingerprint wherever you share your email address, so that people can double-check that they have the correct public key when they download yours from a keyserver.

You may also see public keys referred to by a shorter keyID. This keyID is visible directly from the Key Management window. These eight character keyIDs were previously used for identification, which used to be safe, but is no longer reliable. You need to check the full fingerprint as part of verifying you have the correct key for the person you are trying to contact. Spoofing, in which someone intentionally generates a key with a fingerprint whose final eight characters are the same as another, is unfortunately common.

Important: What To Consider When Signing Keys

Before signing a person's key, you need to be confident that it actually belongs to them, and that they are who they say they are. Ideally, this confidence comes from having interactions and conversations with them over time, and witnessing interactions between them and others. Whenever signing a key, ask to see the full public key fingerprint, and not just the shorter keyID. If you feel it's important to sign the key of someone you've just met, also ask them to show you their government identification, and make sure the name on the ID matches the name on the public key.

Advanced

Master the Web of Trust. Unfortunately, trust does not spread between users the way many people think. One of the best ways to strengthen the GnuPG community is to deeply understand the Web of Trust and to carefully sign as many people's keys as circumstances permit.

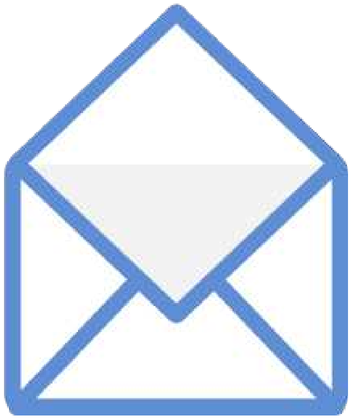
Section #6: Use It Well

Everyone uses GnuPG a little differently, but it's important to follow some basic practices to keep your email secure. Not following them, you risk the privacy of the people you communicate with, as well as your own, and damage the Web of Trust.

When Should I Encrypt? When Should I Sign?

The more you can encrypt your messages, the better. If you only encrypt emails occasionally, each encrypted message could raise a red flag for surveillance systems. If all or most of your email is encrypted, people doing surveillance won't know where to start. That's not to say that only encrypting some of your email isn't helpful -- it's a great start and it makes bulk surveillance more difficult.

Unless you don't want to reveal your own identity (which requires other protective measures), there's no reason not to sign every message, whether or not you are encrypting. In addition to allowing those with GnuPG to verify that the message came from you, signing is a non-intrusive way to remind everyone that you use GnuPG and show support for secure communication. If you often send signed messages to people that aren't familiar with GnuPG, it's nice to also include a link to this guide in your standard email signature (the text kind, not the cryptographic kind).



Be Wary Of Invalid Keys

GnuPG makes email safer, but it's still important to watch out for invalid keys, which might have fallen into the wrong hands. Email encrypted with invalid keys might be readable by surveillance programs.

In your email program, go back to the first encrypted email that Edward sent you. Because Edward encrypted it with your public key, it will have a green checkmark at the top "OpenPGP" button.

When using GnuPG, make a habit of glancing at that button. The program will warn you there if you get an email signed with a key that can't be trusted.

Copy Your Revocation Certificate To Somewhere Safe

Remember when you created your keys and saved the revocation certificate that GnuPG made? It's time to copy that certificate onto the safest storage that you have -- a flash drive, disk, or hard drive stored in a safe place in your home could work, not on a device you carry with you regularly. The safest way we know is actually to print the revocation certificate and store it in a safe place.

If your private key ever gets lost or stolen, you'll need this certificate file to let people know that you are no longer using that keypair.

Important: Act Swiftly If Someone Gets Your Private Key

If you lose your private key or someone else gets a hold of it (say, by stealing or cracking your computer), it's important to revoke it immediately before someone else uses it to read your encrypted email or forge your signature. This guide doesn't cover how to revoke a key, but you can follow these instructions. After you're done revoking, make a new key and send an email to everyone with whom you usually use your key to make sure they know, including a copy of your new key.

Webmail And Gnupg

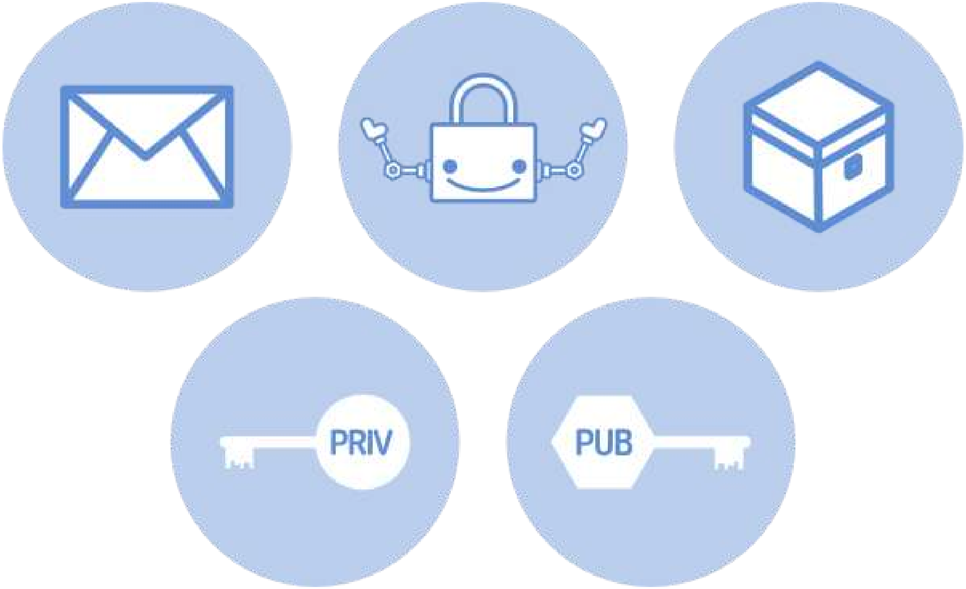
When you use a web browser to access your email, you're using webmail, an email program stored on a distant website. Unlike webmail, your desktop email program runs on your own computer. Although webmail can't decrypt encrypted email, it will still display it in its encrypted form. If you primarily use webmail, you'll know to open your email client when you receive a scrambled email.

Make Your Public Key Part Of Your Online Identity

First add your public key fingerprint to your email signature, then compose an email to at least five of your friends, telling them you just set up GnuPG and mentioning your public key fingerprint. Link to this guide and ask them to join you. Don't forget that there's also an awesome infographic to share.

Start writing your public key fingerprint anywhere someone would see your email address: your social media profiles, blog, Website, or business card. (At the Free Software Foundation, we put ours on our staff page.) We need to get our culture to the point that we feel like something is missing when we see an email address without a public key fingerprint.

Section #7: Next Steps



You've now completed the basics of email encryption with GnuPG, taking action against bulk surveillance. These next steps will help make the most of the work you've done.

Join The Movement

You've just taken a huge step towards protecting your privacy online. But each of us acting alone isn't enough. To topple bulk surveillance, we need to build a movement for the autonomy and freedom of all computer users. Join the Free Software Foundation's community to meet like-minded people and work together for change.

GNU Social

Mastodon

Twitter

Read why GNU Social and Mastodon are better than Twitter, and why we don't use Facebook.

Bring Email Self-defense To New People

Understanding and setting up email encryption is a daunting task for many. To welcome them, make it easy to find your public key and offer to help with encryption. Here are some suggestions:

* # Lead an Email Self-Defense workshop for your friends and community, using our teaching guide.

* # Use our sharing page to compose a message to a few friends and ask them to join you in using encrypted email. Remember to include your GnuPG public key fingerprint so they can easily download your key.

* # Add your public key fingerprint anywhere that you normally display your email address. Some good places are: your email signature (the text kind, not the cryptographic kind), social media profiles, blogs, Web sites, or business cards. At the Free Software Foundation, we put ours on our staff page.

Protect More Of Your Digital Life

Learn surveillance-resistant technologies for instant messages, hard drive storage, online sharing, and more at the Free Software Directory's Privacy Pack and prism-break.org.

If you are using Windows, Mac OS or any other proprietary operating system, we recommend you switch to a free software operating system like GNU/Linux. This will make it much harder for attackers to enter your computer through hidden back doors. Check out the Free Software Foundation's endorsed versions of GNU/Linux.

Optional: Add more email protection with Tor

The Onion Router (Tor) network wraps Internet communication in multiple layers of encryption and bounces it around the world several times. When used properly, Tor confuses surveillance field agents and the global surveillance apparatus alike. Using it simultaneously with GnuPG's encryption will give you the best results.

To have your email program send and receive email over Tor, install the Torbirdy plugin by searching for it through Add-ons.

Before beginning to check your email over Tor, make sure you understand the security tradeoffs involved. This infographic from our friends at the Electronic Frontier Foundation demonstrates how Tor keeps you secure.

Magazine Editor's Note: *The PCLinuxOS Magazine has previously covered the use of OpenPGP to encrypt emails, in the November 2013 article by YouCanToo entitled* ***Mailvelope OpenPGP Encryption For Webmail****. Please feel free to utilize this other article as an additional resource to get up to speed using email encryption with PGP. Between these two articles, we are confident that you should be able to find an email encryption scheme that fits your needs and your situation.*

The PCLinuxOS magazine
Windows Migration Guide
September 2013
The PCLinuxOS magazine
May, 2011
Enlightenment Special Edition
The NEW PCLinuxOS Magazine
Fall 2010
The KDE 4 SC Special Edition
The NEW PCLinuxOS Magazine
Gtk Lightweight Desktops:
Xfce & LXDE Special Edition
November, 2010
The NEW PCLinuxOS Magazine
Command Line Interface Intro
Special Edition
October, 2010
The PCLinuxOS magazine
Openbox Special Edition
March, 2012

Apple & Its Mysterious Privacy Policy

by The Cat

What hides behind Apple's vague and frothy privacy policy?

(photo by chaddlane)

After having delved into Microsoft's 1243 pages long "Privacy Guide", we could not forget its concurrent, the stylish and high-end electronics manufacturer Apple.

If the several and different privacy policies of Microsoft could be compared to a rainforest jungle, then Apple's could be perhaps like a desert. Their Privacy Policy, if downloaded in PDF format, is nine pages in length, of which only three effectively describe what is collected and how they use it. "Great!", you could say, "That proves that Apple collects less data from its users." Well, not exactly. Let's take a look.

They start lecturing on how they care about you and your data, and that all Apple customers in the world will be treated equally regarding their privacy rights. This indeed is very nice, because not all countries have strong privacy regulations like the European Union or Canada, but it is also a pragmatic approach, because it is cheaper to keep one single worldwide policy by their legal department than dozens of them.

Apple also has a "Privacy Governance", where it is stated that they are "committed to respecting human rights, including the right to privacy and freedom of information and expression." Unfortunately, despite the nice wording, equality of treatment and respect of human rights is not necessarily what is practiced by Apple, according to a December 2020 joint letter signed by a coalition of 154 activist groups and rights organizations representing Tibetan, Uyghur, Southern Mongolian, Hongkonger, Taiwanese, and Chinese people. They declare that:

… simply writing a policy document does not in and of itself constitute upholding human rights or taking action for social justice. As you are aware, a number of our coalition members have been engaged in dialogue with Apple […]. The dialogue was entered into in good faith, believing that Apple would act with integrity and openness about developing concrete methods of implementation. This now appears to be far from reality given:

- *The Company's lobbying efforts to undermine and make less transparent Apple's responsibilities under the Uyghur Forced Labor Prevention Act, despite statements that Apple is dedicated to the "goal of eradicating forced labor;"*
- *continued repression of freedom of expression in Hong Kong by banning Apple Store employees from publicly supporting the pro-democracy movement and censoring people choosing pro-freedom and pro-democracy slogans for product engraving; and*
- *failure to detail mechanisms for implementing the "commitments" laid out in Apple's Human Rights Policy, specifically the adherence to freedom of information and expression, as well as the right to freedom of association, including for Apple workers.*

Well, well, it doesn't look so nice as stated in Apple's Privacy Governance. But let's analyze their Privacy Policy, to better understand what they are effectively collecting from their customers. On page three, under the title "Personal Data Apple Collects from You", things start to get confusing: they "bifurcate" their policy, indicating a link to another page on the "handling of personal data for certain individual services", while at the same time showing one paragraph further a bulleted list of "information" collected. Why so much confusion in a company that claims to be so transparent?

But we won't be deterred by this! Let's start with the bulleted list. They say: "… we may collect a variety of information, including…" What is this "including"? Does it mean that you may collect other stuff than that? And if so, what?

And then the list goes, full of vague expressions like "such as", "relating to", but never telling exactly what they are collecting. On an item named "Fraud Prevention Information," they say they will collect "… data used to help identify and prevent fraud, including a device trust score." But what data? And what is this "device trust score" and how is it calculated? Do I have access, as an Apple customer, to all my devices' "trust score"? And what do they do with it?

Then there is the section "Health Information", where they say they collect *"data relating to the health status of an individual, including **data related to one's physical or mental health or condition."***

Mental health? From all users? Or only from those participating in the "Health Research Study"? Why does it seem that Apple avoids using plain, direct words to say what they are doing with your data?

"One bite and all your dreams will come true." (photo by cottonbro)

Further, under the title "Personal Data Apple Receives from Other Sources", on the topic "Apple Partners", they state that: *"we may also validate the information you provide – for example, when creating an Apple ID, **with a third party for security."*** The use of "for example" shows that this list is non-exhaustive, and without stating who are those "third parties", nor the way the data is transmitted, how and where it is stored, etc.

With such a frothy speech, there is no useful information we can gather here. Let's try the link to the other page on the "handling of personal data for certain individual services."

And what do we find here? **Another 64 categories** of data collection! Why are they hidden here, and not in Apple's main privacy policy?

Because it is so long, we will comment here just the most important topics:

Apple can read most of your encrypted data in the iCloud

Only some features use end-to-end encryption. Why is this serious? Because, for most data, even when encrypted at Apple's servers, **they are the ones who keep your cryptographic keys**, and most of the activity from all your devices is stored here. It is like keeping all your valuables in the safe of a bank, but having to leave its keys with the bank. Would you trust them? According to Reuters, Apple dropped plans to let iPhone users fully encrypt backups of their devices in the iCloud after the FBI complained that the move would harm investigations.

Apple evaluates your trust according to your phone calls and emails

Remember that strange "device trust score" mentioned in their privacy policy, without any further explanation? Here it is again, hidden under the topic "Apple Music"! But what is it doing here? Well, let's read what it says:

> *To help identify and prevent fraud**, information about how you use your device, including the approximate number of phone calls or emails you send and receive, will be used to compute a device trust score when you attempt a purchase. […]** The scores are stored for a fixed time on our servers.*

In sum, they will evaluate your "trust" according to your phone calls, emails and more (observe the use of the word including), and will store this score on their servers. Is the data encrypted? And for how long is it stored? We don't know. But we can deduce that they know something about your phone calls and emails, otherwise they wouldn't make such a statement. And it seems you cannot access your own score.

Information about your purchases and downloads are stored for roughly ten years

This regards all purchases and downloads from all Apple online stores: App Store, iTunes, Books, etc. The retention period will vary according to the applicable laws from your region. But despite that, they will retain this data for a longer period if you keep your account with them. "So, if I close my account, all data will be deleted, isn't it?" No! It "… may be retained as business records even after you close your account or stop using the App Store." Great, no? But this is not all! They also keep information about your browsing and searches, and associated with your IP address and Apple ID:

> ***… we use information about your browsing, purchases, searches, and downloads. These records are stored with IP address**, a random unique identifier (where that arises), and Apple ID when you are signed in to the App Store or other Apple online stores.*

Apple will give a score about you to app developers

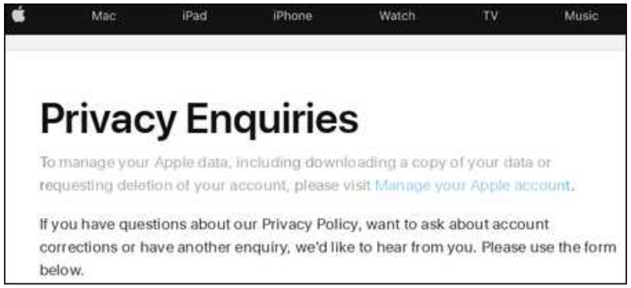
Here it is, hidden in the "Sign in with Apple" topic:

> *For fraud prevention and security reasons, the first time you use Sign in with Apple with a new app, **Apple will share a simple binary score with the developer to give them confidence that you are a real person.** This score is derived from your recent Apple account activity along with abstracted information about your device and device usage patterns.*

As the other topics would only repeat the same platitudes on how they care about you and the same vagueness when it comes to tell what they collect from you, I decided to write them to clarify all my doubts.

Apple Will Not Answer Unpleasant Questions

Using the contact form on their privacy page, I wrote them a message, making basically the questions posed here in this article. I’ve awaited one day, two days, three days… nothing. Perhaps they didn’t receive my message, sometimes those forms don’t work right. Let’s try again. And… nothing.



Privacy Enquiries

To manage your Apple data, including downloading a copy of your data or requesting deletion of your account, please visit Manage your Apple account.

If you have questions about our Privacy Policy, want to ask about account corrections or have another enquiry, we'd like to hear from you. Please use the form below.

“… we’d like to hear from you.” Really?

I must tell you that this is not the first time I wrote to a company asking for clarification on their privacy policies. It is the first time I see messages being completely ignored by a corporation. But, apparently, it is not the first time Apple ducks inconvenient questions. Evan Schumann, from Computerworld, in a report about the company’s sensitive data retention even when the consumer says no, wrote they didn’t directly answer the points he made in an email exchange and declined requests for a phone interview.

Does Apple Care About Privacy More Than Microsoft?

It is not very comfortable to know that a company with access to more than 1.65 billion active devices in the world (of which one billion are active iPhones) operates under such opacity. Its tortuous privacy policy gives the impression that their practices behind their facade of a privacy-loving company could not be so nice. Other elements shed some light on this: the US House Committee on Energy and Commerce stated, in February 2021, that Apple’s App Store privacy labels are *“highly misleading or blatantly false. […] that approximately one third of evaluated apps that said they did not collect data had inaccurate labels.”*

Anyway, they have made some great efforts on de-identification and on processing much of the data inside your own device, instead of doing it on their servers. But they still have access to most of your data stored in the iCloud because it is not encrypted end-to-end, and they still make data collection in several apps an opt-in by default, which is not compliant with the “privacy by default” principle, present in many data privacy regulations.

Microsoft, on the other hand, does not seem to be embarrassed at all about collecting consumers’ data, as we saw in our past article about Microsoft’s privacy policy and their hundreds of pages describing everything they get from users. But I must acknowledge at least one thing: they are pretty clear that they are picking up your data. And a lot. They won’t come with all this frothy language on how they care about you and the like. With Apple, one simply doesn’t know. Their practices are shrouded under such a mystery that you have no idea about what they are doing with your data. And here is the big deal: with Apple, you are paying a premium for devices and services that should be more privacy-respecting. But if they decline to tell you what they do with what they know about your life, would you keep trusting them? Apple keeps a “trust score” about every single user, but it seems it is theirs that is near zero.

PCLinuxOS Recipe Corner Bonus

Italian Beef Kabobs For Two

Servings 4
Unit converter

INGREDIENTS:

1 beef bone-in sirloin or round steak, 3/4 pound, 1 inch thick (340.19 g)
2 garlic cloves, finely chopped
1/4 cup balsamic vinegar (59 ml)
1/4 cup water (59 ml)
1 tablespoon chopped fresh oregano leaves (3.04 g) or 1 teaspoon dried oregano leaves (1.01 g)
2 tablespoons olive or vegetable oil (30 ml)
1 1/2 teaspoons chopped fresh marjoram leaves (3.04 g) or 1/2 teaspoon dried marjoram leaves (1.01 g)
1 teaspoon sugar (4 g)

DIRECTIONS:

1. Remove fat from beef. Cut beef into 1-inch pieces.

2. Mix remaining ingredients in a medium glass or plastic bowl. Stir in beef until coated. Cover and refrigerate, stirring occasionally, at least 1 hour but no longer than 12 hours.

3. Set oven control to broil. Remove beef from marinade; reserve marinade. Thread beef on each of four 10-inch metal skewers, leaving 1/2-inch space between each piece. Brush kabobs with marinade.

4. Place kabobs on a rack in a broiler pan. Broil kabobs with tops about 3 inches from heat 6 to 8 minutes for medium-rare to medium doneness, turning and brushing with marinade after 3 minutes. Discard any remaining marinade.

TIPS:

Although you might be tempted to serve the extra marinade with the cooked kabobs, you should discard any marinade that has been in contact with raw meat. Bacteria from the raw meat could transfer to the marinade.

To speed up prep, omit the garlic, vinegar, water, oregano, oil, marjoram and sugar, and instead, marinate the beef in 2/3 cup purchased Italian dressing in step 2.

If using bamboo skewers, soak in water at least 30 minutes before using to prevent burning.

NUTRITION:

Calories:
144.8

Carbs:
2.2g

Fiber:
0.2g

Sodium:
504.4mg

Protein:
23 g

PCLinuxOS Puzzled Partitions

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

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

When you start a game of Sudoku, some blocks will be 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!

Download Puzzle Solutions Here

S 1	S 1	S 1	L 1	E 1	U 1	M 3
_	_	_	_	_	_	_

Z 10	Y 4	A 1	R 1	F 4	H 4	W 4
_	_	_	_	_	_	_

Triple Word

N 1	N 1	S 1	T 1	U 1	I 1	A 1
_	_	_	_	_	_	_

Double Word

L 1	A 1	N 1	O 1	O 1	O 1	G 2
_	_	_	_	_	_	_

N 1	M 3	U 1	S 1	T 1	A 1	I 1
_	_	_	_	_	_	_

Possible score 226, average score 158.

PCLinuxOS Word Find: August, 2021
On The Beach

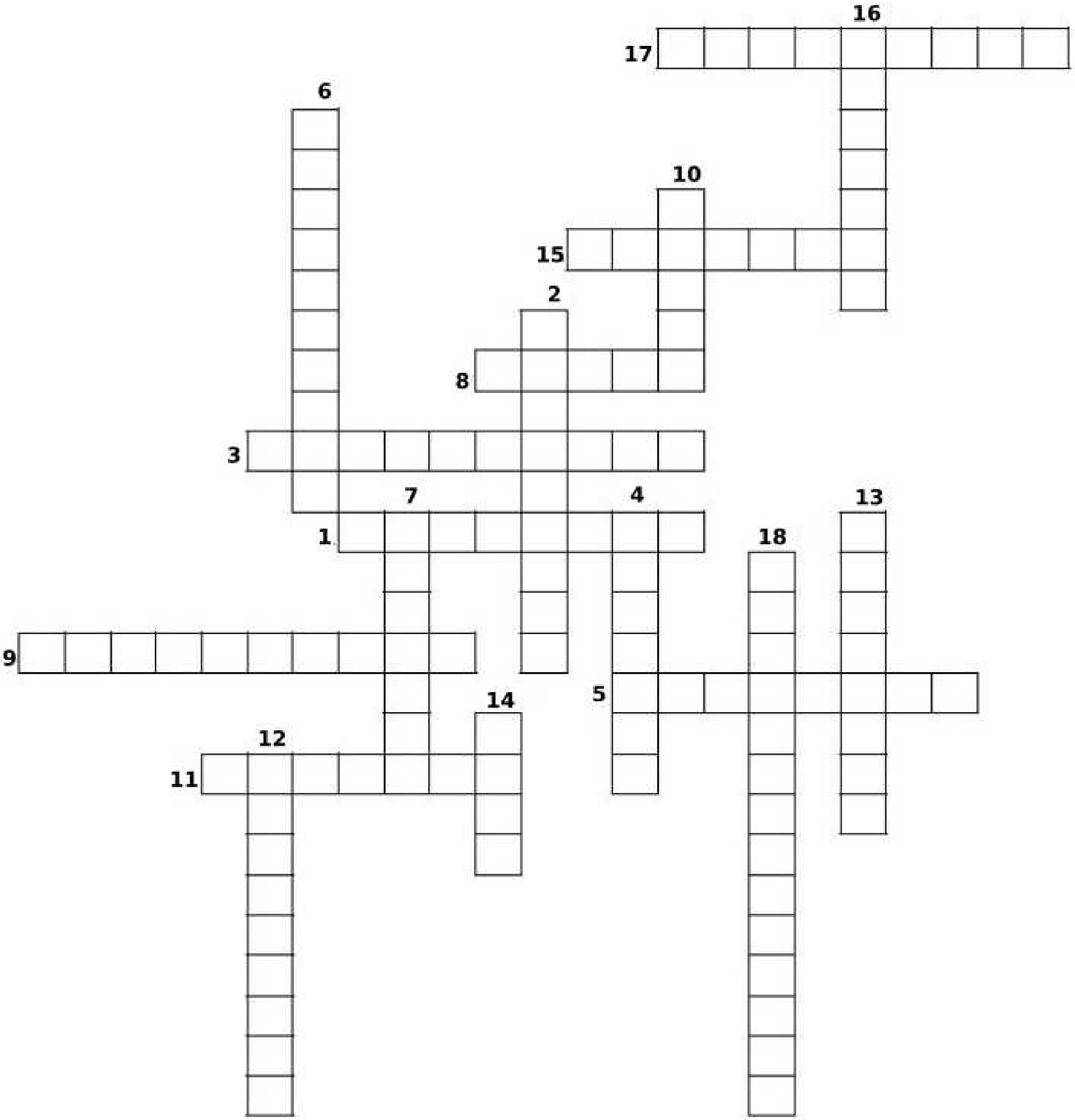
```
A S A N D C A S T L E N E E R C S N U S I I G D L N H T M F
S H O R E B I R D S W P H F C H S K K T L A U P O E G K J W
A V V U W O D Z M M O K A B P V V P W H A R F P T D L V H J
V V V E E G G T A M Y O E L H C Y Q I N A K L V S C M S W L
S T A R F I S H C O S I D L M V R G D C U K Y Y D S C R T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

bathing suit
boardwalk
clam bake
ebb tide
hermit crab
jellyfish
lakeshore
mussels
ocean
pelican
rip current
salt water
sandbar
seagull
seashore
snorkel
sunglasses
tide pool
undertow
wharf

beach
catamaran
conch
hang five
intertidal zone
kelp
mangrove
neap tide
palm tree
reef
sailboat
sand dollar
sandcastle
seashell
shorebirds
starfish
sunscreen
tsunami
waves
yacht

Download Puzzle Solutions Here

On The Beach Crossword



1. Any of various marine echinoderms characteristically having a thick, often spiny body with five arms extending from a central disk.
2. Any of numerous usually free-swimming marine cnidarians, characteristically having a gelatinous, tentacled bell shape.
3. A flat sea-urchin, with a disklike internal skeleton, having five radially symmetric oblong markings.
4. Any of several white, often dark backed birds of the family Laridae, found near coastal areas.
5. An underwater current flowing strongly away from shore.
6. A type of crab species which salvages empty seashells or other portable objects to permanently shelter and protect themselves.
7. A very large ocean wave caused by an underwater earthquake or volcanic eruption.
8. The shore of a body of water, especially when sandy or pebbly.
9. A strong flow of surface water, away from the shore, that returns water from incoming waves.
10. Any of various tropical marine gastropod mollusks chiefly of the family Strombidae, having a large spiral shell often with a flared lip.
11. The period between high tide and the next low tide in which the sea is receding.
12. A promenade, especially of planks, along a beach or waterfront.
13. The tide which occurs just after the first and third quarters of the moon, when there is least difference between high tide and low tide.
14. A strip or ridge of rocks, sand, or coral that rises to or near the surface of a body of water.
15. A breathing apparatus for swimmers and surface divers that allows swimming or continuous use of a face mask without lifting the head to breathe.
16. Any of various marine bivalve mollusks that attach to hard surfaces in intertidal areas.
17. A boat with two parallel hulls or floats, especially a light sailboat with a mast mounted on a transverse frame joining the hulls.
18. The area where the ocean meets the land between high and low tides.

Download Puzzle Solutions Here

Mixed-Up-Meme Scrambler

Docile
ETEGNL ___ ___ ___ □ ___ ___

Visitor
ETGSU □ ___ □ ___ ___

Deceit
RIFGT ___ ___ □ ___ ___

Leather
CHIODWE ___ ___ □ □ ___ ___ ___

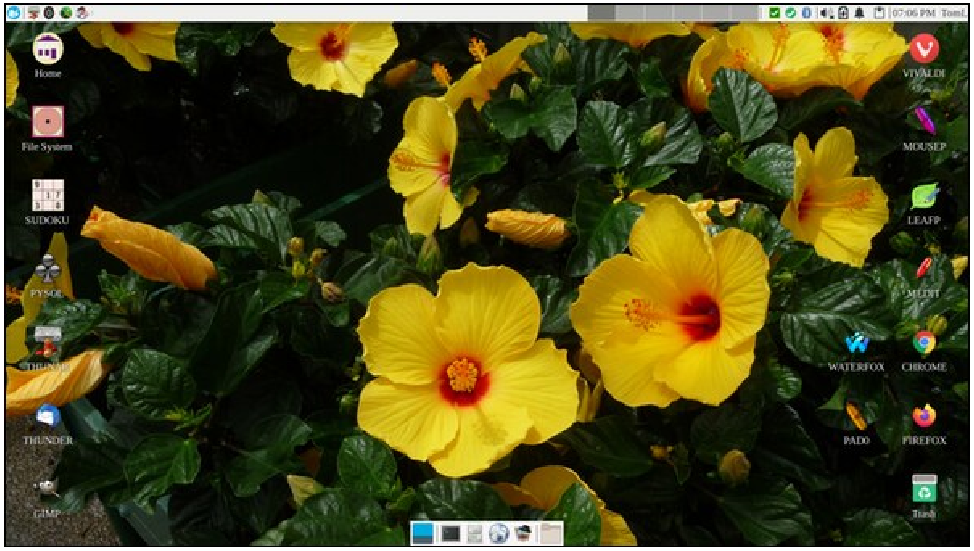
I always bet on PCLinuxOS.
It has the right

___ ___ ___ ___ ___ ___ .

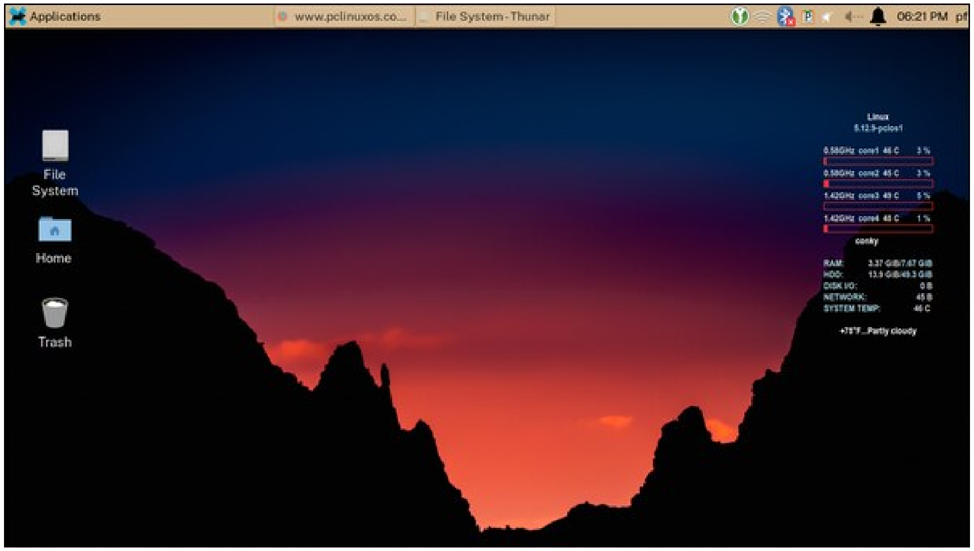
Use the clues to unmix the letters to make a new word. Remix the letters in the red boxes to solve the puzzle.

Download Puzzle Solutions Here

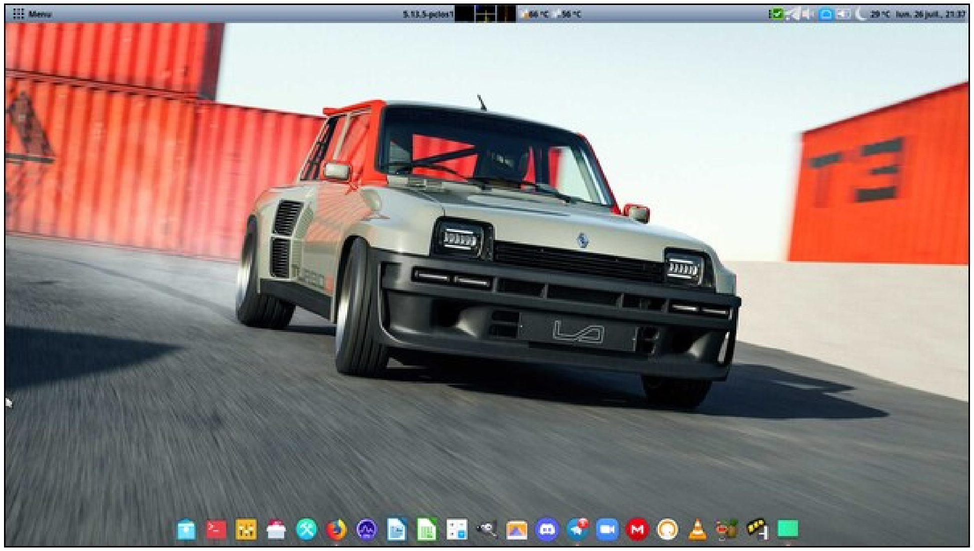
More Screenshot Showcase



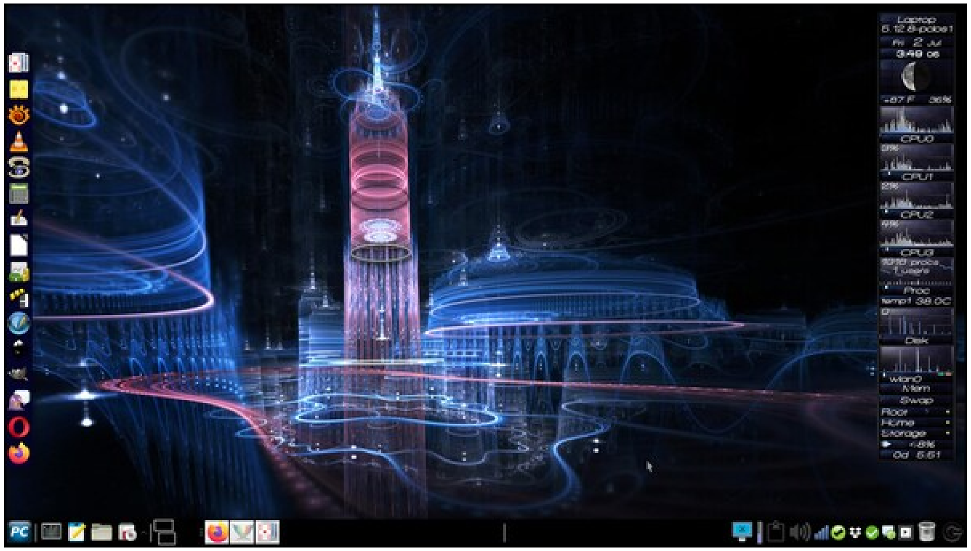
Posted by DrMop, July 21, 2021, running Xfce.



Posted by Yankee, July 16, 2021, running Xfce.



Posted by monbureaulinux, July 26, 2021, running Mate.



Posted by Meemaw, July 2, 2021, running Xfce.