How to Sanitize EXIF Data From Your Pictures

Linux Exif Data and Personal Security

When you take pictures, be it with your cell phone or with your digital camera, the software adds data to the pictures. This data is called the Exif data. If your camera supports it, and if you have it enabled, it will encode all sorts of private data along with your image data.

Needless to say, this is a potential privacy nightmare and people have not only been doxxed this way but people have ended up in jail because of leaving the data in their photos. Now, frankly, if you're taking images that'd get you tossed into jail, I'm pretty much okay with that. For the rest of you, read on…

First, install *exiftool* from your default repositories. If you're using apt, it's quite simple and almost certainly in your default repositories.

[code]sudo apt install exiftool[/code]

Now, let's make it work. Open your *.bash_aliases* file, assuming you have one, and add the following line:

[code]alias picclean="exiftool -overwrite_original -all= *.png && exiftool -overwrite_original -all= *.jpg && echo $PWD 'images cleaned for privacy sake!'"[/code]

Now, reload your aliases with:

[code]source ~/.bash_aliases[/code]

To use this, open the directory that houses the photos you want to share with your terminal and just enter:

[code]picclean[/code]

That will clean all your .png and .jpg files. That's also enough information for you to customize it for your system, should you have a different configuration than I.

HSTS Preload

Seeing as the site is hosted on a Linux server, I'll go ahead and document this. This is how to set up HSTS Preload for your website, by using .htaccess.

If you want to get your site hard-coded into Google Chrome as an "HTTPS Only" site, it's actually relatively easy – once you know how to do it. You can verify that this site is listed here.

Open your site with your favorite FTP application, I prefer Filezilla. Make sure that you've set it to show hidden files. (Files prefaced with a period are hidden files by default.) Edit your *.htaccess* and add the following:

[code]<IfModule mod_headers.c>
Header set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" env=HTTPS
</IfModule>[/code]

Save your file to your server and check your site for yourself.

Why do this? It's added security for your visitors and it's quite probable that Google has a preference for sites who have

taken the time to do so. That may lead to more traffic and happier traffic because they know your site is using HTTPS.

Removing Snap Apps

So many questions are answered by telling people to switch from their snap apps to regularly installed versions of the program. This is how you remove and disable them.

Fortunately, removing and disabling them is quite simple.

[code]sudo apt purge snapd
sudo rm -rf ~/snap
sudo rm -rf /var/snap
sudo rm -rf /var/lib/snapd
sudo reboot[/code]

That will not only disable the snaps and prevent you from installing them, it will also remove any that you have already installed. This will shave some time off your boot and save a tiny amount of system resources.