



Full Circle

THE INDEPENDENT MAGAZINE FOR THE UBUNTU LINUX COMMUNITY

ISSUE #155 - March 2020



Photo: Elicus
(Flickr.com)



RAWTHERAPEE



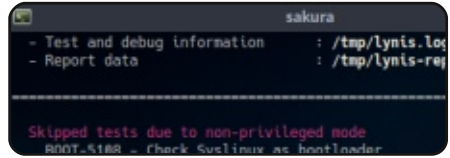
MORE SOFTWARE FOR PHOTOGRAPHERS

Full Circle Magazine is neither affiliated with, nor endorsed by, Canonical Ltd.

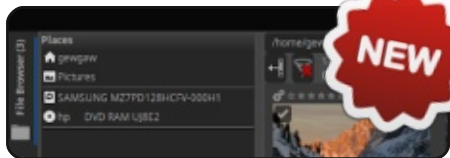
HowTo



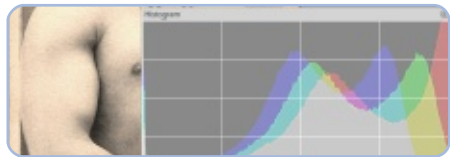
Python p.21



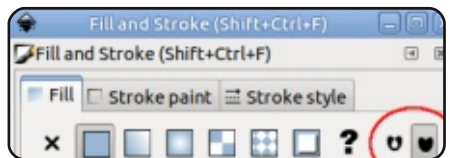
Ubuntu & Security p.26



Rawtherapee p.28



Krita For Old Photos p.35



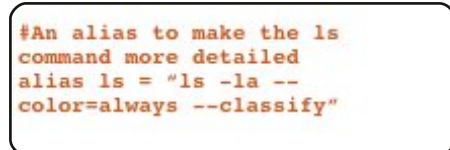
Inkscape p.32

Graphics

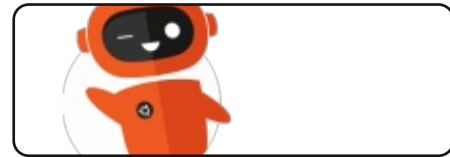


Full Circle

THE INDEPENDENT MAGAZINE FOR THE UBUNTU LINUX COMMUNITY



Command & Conquer p.19



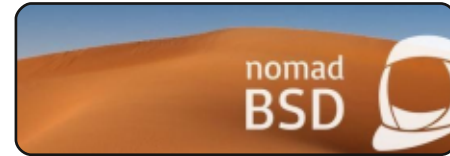
Ubuntu Devices p.XX



My Story p.XX



Q&A p.51



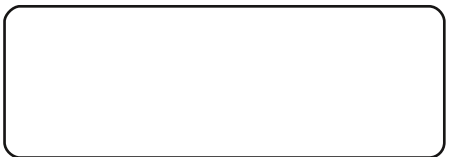
Linux Loopback p.40



The Daily Waddle p.44



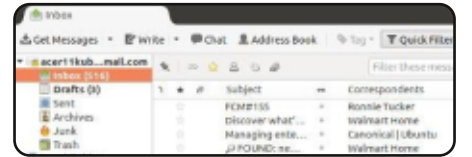
Letters p.XX



XX p.XX



Linux News p.04



Everyday Ubuntu p.41



My Opinion p.45



Review p.48



Ubuntu Games p.55



The articles contained in this magazine are released under the Creative Commons Attribution-Share Alike 3.0 Unported license. This means you can adapt, copy, distribute and transmit the articles but only under the following conditions: you must attribute the work to the original author in some way (at least a name, email or URL) and to this magazine by name ('Full Circle Magazine') and the URL www.fullcirclemagazine.org (but not attribute the article(s) in any way that suggests that they endorse you or your use of the work). If you alter, transform, or build upon this work, you must distribute the resulting work under the same, similar or a compatible license.

Full Circle magazine is entirely independent of Canonical, the sponsor of the Ubuntu projects, and the views and opinions in the magazine should in no way be assumed to have Canonical endorsement.



WELCOME TO THE LATEST ISSUE OF FULL CIRCLE

We have the usual suspects of Python, Inkscape, and Krita, and if you're worried about security then we have an excellent intro to security from Erik.

If you're a photographer, you might be disheartened by the lack of Darktable. Fear not! Erik has a new series on using Rawtherapee for photography. You can never have enough lenses software.

Elsewhere, SJ has a quick look at nomadBSD, Flash continues with PIM, there's a review of a QNAP NAS drive, and a review of the rather unusual looking game, Asciiiker.

Wherever you are in the world, keep safe in these crazy times!

All the best, and (please!) let us know what you like/dislike.

Ronnie

ronnie@fullcirclemagazine.org



This magazine was created using :



Find Full Circle on:



facebook.com/fullcirclemagazine



twitter.com/#!/fullcirclemag



<http://issuu.com/fullcirclemagazine>



<https://mastodon.social/@fullcirclemagazine>

Weekly News:



<http://fullcirclemagazine.org/feed/podcast>



<http://www.stitcher.com/s?fid=85347&refid=stpr>



<http://tunein.com/radio/Full-Circle-Weekly-News-p855064/>

FCM PATREON : <https://www.patreon.com/fullcirclemagazine>



GOOGLE TESTS FUCHSIA OS: 03/02/2020

Google has made changes to indicate the transition of the Fuchsia operating system to the stage of final internal testing "dogfooding", which implies the use of the product in the daily activities of employees, before bringing it to ordinary users. At this stage, the product is in a state that has already passed basic testing by special quality assessment teams. Before delivering the product to the masses, they additionally conduct a final check on their employees who are not involved in the development.

<https://9to5google.com/2020/02/28/fuchsia-friday-dogfood/>

APACHE COUCHDB 3.0 DOCUMENT MANAGEMENT: 03/02/2020

A distributed document-oriented database Apache

CouchDB 3.0 (a NoSQL-system), was released. The source code for the project is distributed under the Apache 2.0 license.

The Couch Replication Protocol lets your data flow seamlessly between server clusters to mobile phones and web browsers, enabling a compelling offline-first user-experience while maintaining high performance and strong reliability. CouchDB comes with a developer-friendly query language, and optionally MapReduce for simple, efficient, and comprehensive data retrieval.

<https://blog.couchdb.org/2020/02/26/3-0/>

CHROME OS 80 RELEASE 03.03.2020

Chrome OS 80 operating system based on the Linux kernel, upstart system manager, ebuild / portage assembly tools, open components, and the Chrome 80 web browser has been released .

The user environment of Chrome OS is limited to a web browser, and instead of standard programs, web applications. However, Chrome OS includes a full multi-window interface, a desktop and a taskbar. Chrome OS 80 builds are available for most current Chromebooks. Enthusiasts builds are available for regular computers with x86, x86_64 and ARM processors. Source code distributed licensed under Apache 2.0.

Initially, the release was scheduled for February 11, but was postponed.

<https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-chrome-os.html>

MASS REVOCATION OF LET'S ENCRYPT CERTIFICATES: 03.03.2020

The community-based Let's Encrypt Certification Authority, a non-profit certification center that provides certificates for everyone, has warned of the

upcoming revocation of many previously issued TLS / SSL certificates. Of the 116 million Let's Encrypt certificates currently in force, a little more than 3 million (2.6%) will be revoked, of which approximately 1 million are duplicates tied to one domain (the error mainly affected very frequently updated certificates, so there are many duplicates). The review is scheduled for the fourth of March, (the exact time has not yet been determined)

<https://community.letsencrypt.org/t/revoking-certain-certificates-on-march-4/114864>

DRAGONFLY BSD 5.8 OPERATING SYSTEM RELEASE: 03.03.2020

The release of DragonFlyBSD 5.8 , a hybrid kernel operating system created in 2003 for the alternative development of the FreeBSD 4.x branch, is available. Among the features of DragonFly

BSD are the distributed versioned HAMMER file system, support for loading "virtual" system cores as user processes, the ability to cache FS data and metadata on SSD drives, contextual variant symbolic links, the ability to freeze processes while maintaining their state on drive, a hybrid kernel using lightweight threads (LWKT).

<http://lists.dragonflybsd.org/pipermail/users/2020-March/358432.html>

NGINX 1.17.9 AND NJS 0.3.9 RELEASE: 03/04/2020

The main branch of nginx 1.17.9 has been updated, in which the development of new features continues (in the parallel supported stable branch 1.16, only changes related to the elimination of serious bugs and vulnerabilities are considered).

Additionally, there was a release of njs 0.3.9, the JavaScript interpreter for the nginx web server. The njs interpreter implements ECMAScript standards and allows you to extend nginx's

query processing capabilities using scripts in the configuration. Scripts can be used in the configuration file to determine the extended logic for processing requests, forming a configuration, dynamically generating a response, modifying a request / response, or quickly creating stubs to solve problems in web applications.

<http://mailman.nginx.org/pipermail/nginx-announce/2020/000265.html>

SAMBA RELEASE 4.12.0: 03/04/2020

The release of Samba 4.12.0, the continued development branch of Samba 4, with a full-fledged implementation of a domain controller and Active Directory service, compatible with the implementation of Windows 2000 and capable of servicing all versions of Windows-clients supported by Microsoft, including Windows 10 is out. Samba 4 is a multifunctional server product, which also provides the implementation of a file server, print service, and authentication server (winbind).

<https://lists.samba.org/archive/samba-announce/2020/000514.html>

NEW VERSION OF CURL 7.69: 03/05/2020

A new version of curl, 7.69.0, which provides the ability to flexibly generate a request by setting parameters such as cookie, user_agent, referer and any other headers, is out. cURL supports HTTP, HTTPS, HTTP / 2.0, SMTP, IMAP, POP3, Telnet, FTP, LDAP, RTSP, RTMP and other network protocols. At the same time, an update was released in parallel to the libcurl library, which provides an API for using all curl functions in programs in languages such as C, Perl, PHP, Python.

The release adds a new backend to support the SSH protocol, made using the wolfSSH library. The backend allows you to transfer data using SFTP with minimal overhead, which makes it possible to use it in tiny-curl collections for embedded systems. SCP is not yet supported in the added backend (use the old libssh backend for SCP).

<https://curl.haxx.se/mail/archive-2020-03/0004.html>

APACHE NETBEANS 11.3 IDE RELEASE: 03/05/2020

The Apache Software Foundation Organization has released their new IDE, NetBeans 11.3. This is the fifth release by the Apache Foundation after the transfer of NetBeans code by Oracle. The first release after the project was transferred from the incubator to primary Apache projects. The release contains support for the Java SE, Java EE, PHP, JavaScript, and Groovy programming languages.

The expected integration of C / C++ language support from version 11.3 of the code base provided by Oracle has been postponed to the next release. Everything related to the development of projects in C and C++ are ready, but the code is not yet integrated. Before built-in support, plug-ins are available. The release of Apache NetBeans 12, which will be accompanied as part of an extended support cycle

(LTS) is planned for April 2020.

<https://blogs.apache.org/netbeans/entry/announce-apache-netbeans-11-3>

INTEL CHIPSET VULNERABILITY TO EXTRACT PLATFORM ROOT KEY:

03/05/2020

Researchers from Positive Technologies identified a vulnerability (CVE-2019-0090), which allows physical extraction of the platform root key (Chipset key), which is used as the “root of trust” for authenticating various components of the platform, including TPM (Trusted Platform Module) firmware) and UEFI.

The vulnerability is caused by a bug in the hardware and in the Intel CSME (Converged Security and Manageability Engine) firmware, which is located in the boot ROM. This does not allow fixing of the problem in already used devices. Due to the presence of a window during the restart of Intel CSME (for example, when waking up from sleep mode), manipulating the DMA, you can

write data to Intel CSME static memory and change the already initialized Intel CSME memory page tables to intercept execution, extract the platform key and receive control over the generation of encryption keys for Intel CSME modules. Details of exploitation of the vulnerability are planned to be published later.

In addition to extracting the key, the error also allows code execution at the zero privilege level of the Intel CSME. The problem affects most Intel chipsets released in the last five years, but in the 10th generation of processors (Ice Point) the problem no longer appears. Intel became aware of the problem about a year ago and in May 2019 firmware updates were released that, although they cannot change the vulnerable code in the ROM, they are trying to block possible vectors at the level of individual Intel CSME modules.

<https://www.ptsecurity.com/ru-ru/about/news/neustranimaya-uyazvimost-v-chipsetah-intel-ugrozhaet-rabochim-stanciyam-i-pravoobladatelyam/>

POWERDNS RECURSOR 4.3 AND KNOTDNS 2.9.3

RELEASE:

03/05/2020

The caching DNS server, PowerDNS Recursor v4.3, has been released. PowerDNS Recursor is built on the same code base as the PowerDNS Authoritative Server, but the recursive and authoritative PowerDNS DNS servers are developed as part of different development cycles and released as separate products. The project code is distributed under the GPLv2 license.

The server provides tools for remote statistics collection, supports instant restart, has a built-in engine for connecting handlers in the Lua language. It fully supports DNSSEC, DNS64, RPZ (Response Policy Zones) and allows you to connect blacklists. It is possible to record the results of resolving in the form of BIND zone files. To ensure high performance, modern connection multiplexing mechanisms in FreeBSD, Linux and Solaris (kqueue, epoll, / dev / poll) are used, as well as a high-performance parser for DNS

packets that can handle tens of thousands of parallel requests.

<https://blog.powerdns.com/2020/03/03/powerdns-recursor-4-3-0-released/>

SANDCASTLE PROJECT PREPARES LINUX AND ANDROID BUILDS FOR INSTALLATION ON IPHONE 7:

03/06/2020

Project Sandcastle published a build for Linux and Android. The project is suitable for installation on the iPhone 7 and 7+ . The project also provides limited support for iPod Touch 7G and porting to various iPhone 6, 8, X, 11 and iPod Touch 6G models is ongoing. The software still has a way to go.

<https://projectsandcastle.org/>

AN ERROR IN BIND 9.16 THAT DISRUPTS THE PROCESSING OF TCP CONNECTIONS:

03/06/2020

In the BIND 9.16.0 branch published two weeks ago, a serious error was revealed exhausting the limit on the number of TCP connections. In BIND 9.16, a new network subsystem was proposed, which was transferred to the asynchronous request processing mechanism based on the libuv library. Due to an error in this subsystem, the counter of active TCP connections does not decrease under certain conditions, which leads to an increasing discrepancy between its value and the actual number of connections. After some time, the counter value may reach the set limit on the number of client connections and new TCP requests will cease to be accepted (UDP requests will continue to be processed).

Basically, the problem manifests itself on servers that accept TCP connections from clients on several network

interfaces at once. BIND 9.16 has not yet been released, but a patch has been published to fix the error. As a temporary solution, you can set the limit on the number of connections (option tcp-clients) to a very large value. In addition to BIND 9.16, the problem affects the experimental branch 9.15, starting with the release of 9.15.6, but this branch was originally used only for development and is not focused on production servers.

<https://www.mail-archive.com/bind-announce@lists.isc.org/msg00567.html>

GNU COREUTILS 8.32 BASIC SYSTEM UTILITY LAUNCH:

03/06/2020

After a year of development, a stable version of the GNU Coreutils 8.32 set of basic system utilities is available. It includes programs such as sort, cat, chmod, chown, chroot, cp, date, dd, echo, hostname, id, ln, ls, etc. d.

http://savannah.gnu.org/forum/forum.php?forum_id=9693

SECOND RELEASE OF GLIMPSE, FORK OF THE GIMP GRAPHICS EDITOR:

03/06/2020

The second release of the Glimpse graphics editor has been published. Builds are available for Windows and Linux (so far only in the Flatpak format, but Snap will be available too). Other than correcting errors from the previous release, the addition of new themes for interface design and icons was touted. There were improved translations for non-English-speaking users, removal of the word "gimp", adding settings for choosing a language on the Windows platform, and removing unnecessary "fun" brushes.

The proposed release of Glimpse is based on GIMP 2.10.12, with rebranding, renaming directories and cleaning the user interface. The external dependencies are BABL 0.1.68, GEGL 0.4.16 and MyPaint 1.3.0.

<https://glimpse-editor.org/posts/glimpse-0-1-2-release-notes/>

DEVELOPMENT OF DNF 5 PACKAGE MANAGER AND PACKAGEKIT REPLACEMENT STARTED:

03/06/2020

Daniel Mach of Red Hat announced the start of the development on the DNF 5 package manager, which will port Python-implemented DNF logic to the C++ libdnf library. They plan to begin testing DNF 5 in June during the development of Fedora 33, in October 2020. They plan to add it to the Rawhide repository, and replace DNF 4 with it in February 2021. Maintenance of the DNF 4 branch will continue, as it is used in Red Hat Enterprise Linux 8. The project has reached a state in which it is almost impossible to continue the development of code without compromising compatibility at the API / ABI level. This is mainly due to the loss of relevance of PackageKit and the inability to develop libdnf without changing the "libhif" API. At the same time, despite the intention to change the API, maintaining backward compatibility at command line interface level and API is prioritised.

<https://lists.fedoraproject.org/archives/list/devel@lists.fedoraproject.org/thread/NWSURJRGZAIIMNZJT244DHDPOG2PBQXZ/>

SYSTEMD 245 AVAILABLE WITH PORTABLE HOME DIRECTORIES:

03/06/2020

After three months of development, the release of the systemd 245 system manager is announced. In the new release, new components systemd-homed and systemd-repart are added. Support for portable user profiles in JSON format is included, the ability to define namespaces in systemd-journald is provided and support for the "pidfd" mechanism is added. The project website has been completely redone, where most of the available documentation has been collected and a new logo has been proposed.

<https://lists.freedesktop.org/archives/systemd-devel/2020-March/044119.html>

VULNERABILITY IN PPPD AND LWIP ALLOWING REMOTE CODE EXECUTION WITH ROOT PRIVILEGES:

03/07/2020

A vulnerability was identified in the pppd package (CVE-2020-8597), which allowed it to execute its code by sending specially crafted authentication requests to systems using PPP (Point-to-Point Protocol) or PPPoE (PPP over Ethernet). These protocols are usually used by providers to establish connections via Ethernet or DSL, and are also used in some VPNs (for example, pptpd and openfortivpn).

The issue affects pppd versions 2.4.2 through 2.4.8 inclusive and is fixed in the form of a patch. The vulnerability also affects the lwIP stack, but EAP support is not enabled in the default configuration in lwIP.

<https://www.kb.cert.org/vuls/id/782301/>

MIN 1.13 WEB BROWSER PUBLISHED:

03/07/2020

Min 1.13 is out, offering a minimalistic interface, built around the manipulation of the address bar. The browser was created using the Electron platform, which allows you to create stand-alone applications based on the Chromium engine and the Node.js. platform. The Min interface is written in JavaScript, CSS and HTML. The code is licensed under Apache 2.0. Builds are available for Linux, macOS and Windows. The browser has a built-in ad blocking system (EasyList) and a code for tracking visitors, it is also possible to disable the downloading of images and scripts.

<https://github.com/minbrowser/min/releases/tag/v1.13.0>

TWO ATTACKS ON THE CACHE CHANNEL PREDICTION MECHANISM IN AMD PROCESSORS:

03/07/2020

A team of researchers from Graz University of Technology (Austria), conducted a study of AMD-specific hardware optimizations and developed two new third-party channel attack methods that manipulate data leaks during channel prediction in the level one cache of AMD processors. Methods can be used to reduce ASLR protection, restore keys in vulnerable AES implementations, and increase Specter attack efficiency.

Problems were identified in the implementation of the channel predictor mechanism (way predictor) in the data cache of the first level of the CPU (L1D), which is used to predict which channel of the cache reflects a specific memory address. The optimization used in AMD processors is based on the verification of μ tags (μ Tag). μ Tag is calculated by applying a specific hash function to the virtual address. During operation, the channel prediction mechanism uses μ Tag to determine the cache channel from the table. Thus, μ Tag allows the processor to limit itself to accessing only a specific channel, without enumerating all the options, which significantly

reduces CPU power consumption.

<https://mlq.me/download/takeaway.pdf>

APT 2.0 PACKAGE MANAGER RELEASED:

03/08/2020

The release of the package management tool APT 2.0 (Advanced Package Tool), developed by the Debian project, is available. APT is also used in some distributions based on the rpm package manager, such as PCLinuxOS and ALT Linux. The new branch has incorporated the changes in the development of the experimental branch 1.9.x. In the near future, the new release will be integrated into the Debian Unstable branch and into the

Ubuntu package base (experimental branch 1.9 was used in Ubuntu 19.10).

<https://blog.jak-linux.org/2020/03/07/apt-2.0/>

ZORIN OS 15.2

DISTRIBUTION RELEASE:

03/09/2020

Zorin OS 15.2 Linux, a distribution based on the Ubuntu 18.04.4 base is out. The distribution's target audience is novice users who are used to working in Windows. To control the design, the distribution offers a special configurator that allows you to mimic different versions of Windows, and the software selection includes programs that are close to the programs that

Windows users are used to. The bootable iso-image is 2.3 GB in size (two desktop environments are available - the usual one based on GNOME and "Lite" with Xfce).

<https://zoringroup.com/blog/2020/03/05/zorin-os-15-2-is-released-harder-better-faster-stronger/>

VULNERABILITY IN TIMESHIFT THAT COULD ELEVATE ITS PRIVILEGES IN THE SYSTEM:

03/09/2020

A vulnerability has been identified in the Timeshift application (CVE-2020-10174), allowing a local user to execute code with root privileges. Timeshift is a backup system that uses rsync

FULL CIRCLE WEEKLY NEWS



Join our new host Leo Chavez as he presents you with a short podcast (<10min) with just the news. No chit-chat. No time wasting. Just the latest FOSS/Linux/ Ubuntu news.

RSS:

<http://fullcirclemagazine.org/feed/podcast>



DistroWatch.com

Put the fun back into computing. Use Linux, BSD.

with hard links or Btrfs snapshots to implement functionality similar to System Restore on Windows and Time Machine on macOS. The program is included in the repositories of many distributions and is used by default in PCLinuxOS and Linux Mint. The vulnerability is fixed in Timeshift 20.03 release .

<https://www.openwall.com/lists/oss-security/2020/03/06/3>

MERGER OF FREENAS AND TRUENAS PROJECTS

ANNOUNCED:

03/09/2020

Ixsystems announced the unification of its products for the rapid deployment of network storage (NAS, Network-Attached Storage). The free FreeNAS distribution will be merged with the TrueNAS commercial project , expanding the capabilities of FreeNAS for enterprises and comes pre-installed on storage systems manufactured by Ixsystems.

The combination will speed up development and shorten the

release cycle to 6 months, strengthen quality control, synchronize development with FreeBSD to provide more rapid support for new equipment, simplify documentation, unify sites, simplify migration between commercial and free distributions, accelerate the transition to OpenZFS 2.0 to base "ZFS on Linux".

<https://www.ixsystems.com/blog/freenas-truenas-unification/>

4MLINUX 32.0

DISTRIBUTION RELEASE:

03/10/2020

4 MLinux 32.0, a minimalist custom distribution that is not an offshoot of other projects and uses a graphical environment based on JWM, is ready. 4MLinux can be used not only as a live environment for playing multimedia files and solving user problems, but also as a recovery system and a platform for launching LAMP servers (Linux, Apache, MariaDB and PHP). The size of the iso-image is only 830 MB (i686, x86_64).

The new release implements support for decoding video in the AV1 format (via dav1d from FFmpeg). The PCManFM file manager provides the ability to create thumbnails for videos and documents in PS and PDF formats. Editors included: SciTE, GNU nano and mg (MicroGnuEmacs). As a downloadable add-on, Vim is available (with gVim). Lots of updated packages in this release.

<https://4mlinux-releases.blogspot.com/2020/03/4mlinux-320-stable-released.html>

THE RELEASE OF THE CONSOLE SCREEN SAVER NEOFETCH 7.0.0:

03/10/2020

N eofetch 7.0.0 utility is available. By default, the program displays the logo of the operating system, which can be replaced with an arbitrary picture (for terminals that support image display) or an ASCII picture. The utility supports about 150 operating systems, from Linux and Windows to Minix, AIX and Haiku. The program is written in Bash and distributed under the MIT license.

The new version adds support for: Proxmox VE, BlackArch, Neptune, Obarun, Drauger OS, macOS Catalina, ArchStrike, Cucumber Linux, EuroLinux, Cleanjaro, Septor Linux, Carbs Linux, EndeavourOS and T2. They also added support for the Regolith desktop . The release includes a selection of compact logos.

<https://github.com/dylananaraps/neo-fetch/releases/tag/7.0.0>

POSTGRESQL ANONYMIZER 0.6, AN EXTENSION FOR ANONYMIZING DATA IN A DBMS:

03/10/2020

A new release of the PostgreSQL Anonymizer project is available, which solves the problem of hiding or replacing confidential data. Data can be hidden on the fly based on specially defined rules and lists. The code is distributed under the PostgreSQL license.

For example, using the add-on in question, you can provide access

to the database to third parties, such as, third-party business intelligence services, automatically denying them access to phone numbers and credit cards, or using more sophisticated methods, such as changing customer and company names to fictitious information. In addition to performing anonymization when connecting directly to the DBMS, there is a mode for creating anonymized SQL dumps

<https://www.postgresql.org/about/news/2017/>

RELEASE OF HOBBITS 0.21, A VISUALIZER FOR REVERSE ENGINEERING BINARY FILES: 03/10/2020

Hobbits 0.21 project is out , a graphical interface for the analysis, processing and visualization of binary data in reverse engineering. The code is written in C ++ using the Qt library and is distributed under the MIT license.

Parsing, processing and visualization are connected via plugins, which can be selected

depending on the type of data being analyzed. Plugins are available for the classic hexadecimal display, binary and ASCII representations, bitwise and byte-by-bit rasterization (each pixel is associated with a bit or byte) and character rasterization. For data analysis, plugins are offered for searching and navigating data, highlighting standard templates and headers, defining blocks based on regular expressions.

<https://github.com/Mahlet-Inc/hobbits/releases/tag/v0.21.0>

MORE INTEL WOES WITH LVI: 03/11/2020

There is a new class of attacks LVI (Load the Value Injection, the CVE-2020-0551) speculative execution in the CPU, which can be used for the diversion of keys and sensitive data from the Intel SGX enclave and other processes.

The new attack class is based on manipulations with the same microarchitectural structures as in the MDS (Microarchitectural Data Sampling), Specter, and Meltdown

attacks . At the same time, new attacks are not blocked by existing methods of protection against Meltdown, Specter, MDS and other similar attacks. Effective LVI protection requires hardware changes to the CPU. Software mitigations, by adding the LFENCE instruction by the compiler after each load operation from memory and replacing the RET instruction with POP, LFENCE and JMP, is just too much overhead - according to researchers, full software protection will lead to between 2-19 times performance degradation.

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00334.html>

WEBKITGTK 2.28.0 BROWSER ENGINE AND EPIPHANY 3.36 WEB BROWSER RELEASE: 03/11/2020

The release of the new stable branch of WebKitGTK 2.28.0, is out. WebKitGTK allows you to use all the features of WebKit through

a GNOME-oriented programming interface based on GObject . It can be used to integrate web-content processing tools into any application, from specialized HTML / CSS parsers, to create full-featured web browsers. Well-known projects using WebKitGTK are Midori and the standard GNOME browser (Epiphany) .

<https://webkitgtk.org/2020/03/10/webkitgtk2.28.0-released.html>

SDL 2.0.12 MULTIMEDIA LIBRARY RELEASE: 03/11/2020

The release of the SDL 2.0.12 library (Simple DirectMedia Layer), aimed at simplifying the writing of games and multimedia applications, has been announced . The SDL library provides tools such as hardware-accelerated 2D and 3D graphics output, input processing, audio playback, 3D output via OpenGL / OpenGL ES, and many other related operations. The library is written in C and distributed under the zlib license. To use the SDL features in projects in various programming languages, binders are provided.

<https://discourse.libsdl.org/t/sdl-2-0-12-released/27318>

GNOME 3.36 USER ENVIRONMENT RELEASE:

03/11/2020

After six months of development GNOME 3.36 DE is out . Compared with the previous release, about 24 thousand changes were made, in which 780 developers took part. To quickly evaluate the capabilities of GNOME 3.36, specialized live builds based on openSUSE and Ubuntu have been released .

<https://www.mail-archive.com/devel-announce-list@gnome.org/msg00999.html>

VALVE RELEASES PROTON 5.0-4, A PACKAGE FOR RUNNING WINDOWS GAMES ON LINUX:

03/11/2020

Valve has published the release of the Proton 5.0-4 project , which is based off the Wine project

and is aimed at ensuring that games created for Windows, launch on Linux. Project developments are distributed under the BSD license.

Proton allows you to directly run games that are only available for Windows on your Linux client. The package includes an implementation of DirectX 9/10/11 (based on the DXVK package) and DirectX 12 (based on vkd3d). The Vulkan API, provides improved support for game controllers and the ability to use full-screen mode regardless of games screen resolutions. To increase the performance of multi-threaded games, the " esync " (Eventfd Synchronization) and " futex / fsync " mechanisms are supported .

<https://github.com/ValveSoftware/Proton/releases/tag/proton-5.0-4>

DEBIAN 8 WILL BE SUPPORTED FOR MORE THAN 5 YEARS:

03/11/2020

The LTS Team, responsible for generating updates for the Debian LTS branches , announced

the possibility of receiving updates for the Debian 8 "Jessie" after the completion of the regular five-year maintenance cycle. Originally they planned to stop supporting the Debian 8 LTS branch in July 2020, but Freexian expressed its readiness to release updates on its own with the elimination of package vulnerabilities as part of the Extended LTS program .

Additional support will cover a limited set of packages and apply only to the amd64 and i386 architectures (possibly arm). Support will not cover packages such as the Linux 3.16 kernel (the 4.9 kernel backported from Debian 9 "Stretch" will be offered), openjdk-7 (openjdk-8 will be offered) and tomcat7 (maintenance will last until March 2021). Updates will be distributed through an external repository maintained by Freexian. Access will be free for all, and the range of supported packages will depend on the total number of sponsors and packages that interest them.

<https://raphaelhertzog.com/2020/03/11/keeping-debian-8-jessie-alive-for-longer-than-5-years/>

MOZILLA WILL HELP IN UPDATING THE KAIOS PLATFORM (FORK OF FIREFOX OS):

03/12/2020

Mozilla and KaiOS Technologies announced a collaboration aimed at updating the browser engine used in the KaiOS mobile platform. KaiOS continues to develop the Firefox OS mobile platform and is currently used on approximately 120 million devices sold in more than 100 countries. The problem is that KaiOS continues to use an outdated browser engine, corresponding to Firefox 48, that ceased 2016. This engine is outdated, does not support many current web-technologies and does not provide proper security.

The purpose of cooperation with Mozilla is to transfer KaiOS to the new Gecko engine and keep it up to date, including regular publication of patches to eliminate vulnerabilities. Work also involves optimizing the performance of the platform and related services and applications. All changes and improvements will be published

under the free MPL (Mozilla Public License).

<https://www.kaiostech.com/press/kaios-technologies-and-mozilla-partner-to-enable-a-healthy-mobile-internet-for-everyone/>

GENODE PROJECT RELEASES SCULPT 20.02 GENERAL PURPOSE OS:

03/12/2020

The developers of the open microkernel operating system Genode OS Framework have released the Sculpt operating system yesterday. As part of the Sculpt project, Genode-based technology is developing a general-purpose operating system that can be used by ordinary users to perform everyday tasks. The source code for the project is distributed under the AGPLv3 license. A 26 MB LiveUSB image is offered for download. It supports systems with Intel processors and graphics with the VT-d and VT-x extensions enabled.

In this new release you will find a file manager working in graphical mode, the processing of an

interactive interface for administration (the system settings editor), support for virtual desktops, and optimization of the performance of the virtual machine monitor (based on VirtualBox). Updated utilities for monitoring system performance, Unix runtime, and GUI components. The release also includes enhancements introduced in the February Genode platform update, such as support for 64-bit i.MX ARM processors and porting of the sound driver from OpenBSD 6.6.

<https://github.com/genodelabs/genode>

TAILS 4.4 AND TOR BROWSER 9.0.6 RELEASE:

03/12/2020

The release of the specialized Tails 4.4 distribution (The Amnesic Incognito Live System), based on Debian and designed to provide anonymous access to the internet, is out. All connections except traffic through the Tor network are blocked by default with a packet filter. Encryption is used to store user data in the "save user data mode" between restarts.

The new version of Tor Browser has been updated to release 9.0.6 (at the time of writing the news has not yet been officially announced), synchronized with the Firefox 68.6.0 ESR code base. Also updated are: the Linux kernel 5.4.19, Thunderbird 68.5.0, cURL 7.64.0, evince 3.30.2, Pillow 5.4.1, WebKitGTK 2.26.4, virtualbox 6.1.4. Also adding missing firmware for wireless cards based on Realtek RTL8822BE / RTL8822CE chips.

Addition: Tor Browser 9.0.6 based on Firefox 68.6.0, which also updated NoScript 11.0.15 that stops loading built-in CSS external Fonts in Safe Mode. The developers also warned of a remaining uncorrected error, which made it possible to launch JavaScript code in the "Safest" protection mode. The problem has not yet been resolved, so for those for whom the blocking of JavaScript execution is important, it is recommended, for a while, in about: config to completely block the use of JavaScript in the browser by changing the javascript.enabled parameter in about: config.

https://tails.boum.org/news/version_4.4/index.en.html

DEBIAN 11 PACKAGE BASE FREEZE SCHEDULED FOR NEXT YEAR:

03/12/2020

Debian developers have published a plan to freeze the Debian 11 "Bullseye" release. A Debian 11 release is expected in mid-2021.

On January 12, 2021, the first stage of freezing the package base will begin, within which the transitions will be stopped (updating packages that require dependency corrections for other packages, which will temporarily remove packages from Testing), as well as stopping updating packages needed for assembly (build-essential).

On February 12, 2021, a soft freezing of the package base will take place, at which the reception of new source packages will be stopped and the ability to re-enable previously deleted packages will be closed.

On March 12, 2021, a hard freeze will be applied before release, in which the process of

transferring key packages and packages without autopkg tests from unstable to testing will be completely stopped and the stage of intensive testing and bug fixing, blocking release will begin. Hard freezing is introduced for the first time and is considered as a necessary intermediate stage before complete freezing, covering all packages. The time of complete freezing is not yet determined.

<https://lists.debian.org/debian-devel-announce/2020/03/msg00002.html>

GCC 9.3 COMPILER SUITE UPDATE:

03/12/2020

A bug fix release of the GCC 9.3 compiler suite is available, with a lot of work done to fix errors, regressive changes and compatibility issues. Compared to GCC 9.2, GCC 9.3 has 157 fixes, mainly related to resolving regressive changes.

<https://www.mail-archive.com/info-gnu@gnu.org/msg02716.html>

ALT P9 STARTER KITS QUARTERLY UPDATE:

03/13/2020

The fourth round of starter kits is available on the Ninth Alt platform, made for i586, x86_64, aarch64 and arm architectures. Releases for MIPS architecture are proposed in versions for the Russian Tavolga and BFK3 systems on the Baikal-T1 CPU's. Owners of Elbrus VK based on 4C and 8C / 1C + processors also have access to a number of starter kits. Starter kits are suitable for starting work with a stable repository for users who prefer to install their own list of application packages to configure their systems. Images include a basic system, one for desktop environments or a set of specialized applications.

<https://getalt.org/ru/starterkits/>

NGINX UNIT 1.16.0 APPLICATION SERVER RELEASE:

03/13/2020

The NGINX Unit 1.16 application

server was released, to ensure the launch of web applications in various programming languages (Python, PHP, Perl, Ruby, Go, JavaScript / Node.js and Java). Under the control of the NGINX Unit, several applications in different programming languages can be run simultaneously, the launch parameters can be changed dynamically without the need to edit configuration files and restart. The code is written in C and distributed under the Apache 2.0 license. If you want to know more, read the initial release notes.

<http://unit.nginx.org/>

RUST 1.42 IS OUT:

03/13/2020

Rust 1.42 system programming language, based on the Mozilla project, is released. The language is focused on safe work with memory, provides automatic memory management and provides means to achieve high concurrency of tasks, without having to use a garbage collector and runtime.

Automatic memory

management in Rust saves the developer from manipulating pointers and protects against problems arising from low-level work with memory, such as accessing a memory area after it was freed, dereferencing null pointers, going out of buffer boundaries, etc. To distribute libraries, ensure assembly, and manage project dependencies, a Cargo package manager is developed that allows you to get the libraries you need for the program in one click. Check out crates.io for more cargo cartes.

<https://blog.rust-lang.org/2020/03/12/Rust-1.42.html>

RED HAT ENTERPRISE LINUX VULNERABILITY REPORT FOR 2019:

03/13/2020

Red Hat has published a report for vulnerabilities identified in Red Hat products during 2019. Over the year, 1313 vulnerabilities were fixed in Red Hat products and services (3.2% more than in 2018), 27 of them were critical problems. In total, the Red Hat security

service in 2019 examined 2714 vulnerabilities covering all possible problems, including open programs that are not part of RHEL or do not appear in RHEL.

Updates to eliminate 98% of critical issues were released within a week, after public information about the vulnerability became known. The largest number of vulnerabilities were fixed in the Linux kernel and packages with browser components.

<https://www.redhat.com/en/blog/evuiewing-vulnerabilities-2019-annual-red-hat-product-security-risk-report>

LOADLIBRARY, A LAYER FOR LOADING WINDOWS DLLS IN LINUX APPLICATIONS:

03/13/2020

Thavis Ormandy, security researcher at Google, is developing a project, LoadLibrary, aimed at porting collected Windows DLL-libraries for use in applications in Linux. The project provides an interlayer library with which you can load a DLL file in PE / COFF format and call the

functions defined in it. The PE / COFF loader is based on the ndiswrapper code. The project code is distributed under the GPLv2 license.

LoadLibrary takes over the functions of loading the library into memory and importing existing characters, providing the Linux application with a dlopen-style API. Pluggable code can be debugged using gdb, ASAN and Valgrind. You can adjust the executable code at runtime by connecting hooks and applying patches (runtime patching). The aim of the project is to organize scalable and efficient distributed fuzzy testing of DLLs in a Linux-based environment. In Windows, conducting fuzzing and coverage testing does not allow for proper performance and often requires launching a separate virtualized instance of Windows, especially when trying to analyze sophisticated products, such as antivirus software, covering work at the kernel level and user space. With the help of LoadLibrary, Google researchers are searching for vulnerabilities in video codecs, antivirus scanners, data decompression libraries, image decoders, etc.

<https://github.com/taviso/loadlibrary>

WINE 5.4 AND WINE STAGING 5.4 RELEASE:

03/14/2020

A pilot release of the open implementation of WinAPI - Wine 5.4 is available. Since the release of version 5.3, 34 error reports have been closed and 373 changes made.

At the same time, the release of the Wine Staging 5.4 project is available, including incomplete or risky patches that are not yet suitable for adoption in the main Wine branch. Compared to Wine, Wine Staging provides 855 additional patches. The new release synchronizes with the Wine 5.4 codebase.

<https://www.winehq.org/announce/5.4>

LIBREELEC 9.2.1 HOME CINEMA DISTRIBUTION UPDATE:

03/14/2020

LibreELEC 9.2.1 project, a fork distribution of OpenELEC home theater, has been published. The user interface is based on the Kodi media center. Images for a USB drive or SD card (32-bit and 64-bit x86, Raspberry Pi 1/2/3/4, various devices based on Rockchip and Amlogic chips) are available for download. In the new version, a section for configuring VPN WireGuard is added to the configurator, and support for working on Raspberry Pi 4 boards is improved (performance and output quality are improved in 1080p and 4K modes).

<https://libreelec.tv/2020/03/libreelec-leia-9-2-1/>

VULNERABILITY IN BLUEZ BLUETOOTH STACK:

03/14/2020

The vulnerability could potentially allow an attacker to gain access to the system. Due to incorrect access control in the implementation of HID and HOGP Bluetooth profiles, the vulnerability allows denial of service or elevation of privileges

when connecting a malicious Bluetooth device without going through the process of binding the device to the host. A malicious Bluetooth device without passing the pairing procedure can impersonate another HID device (keyboard, mouse, game controllers, etc.) or hidden data substitution into the input subsystem.

According to Intel, the problem is in releases of Bluez up to and including v5.52. It is unclear whether the issue affects v5.53, as it has not been publicly announced, but has been available through Git and in the archive since February. Patches for fixing both vulnerabilities were proposed on March 10, and release 5.53 was posted on February 15. Some distro's have not yet been updated (Debian, Ubuntu, SUSE, RHEL, Arch, Fedora).

<https://www.openwall.com/lists/os-security/2020/03/12/4>

OPEN SOURCE SOFTWARE FOUNDATION ANNOUNCED THE ANNUAL AWARD FOR CONTRIBUTION TO THE DEVELOPMENT OF FREE SOFTWARE:

03/15/2020

At the LibrePlanet 2020 conference, which was held online this year due to the coronavirus pandemic, a virtual awards ceremony was held to announce the winners of the annual Free Software Awards 2019. It was established by the Free Software Foundation (FSF) and awarded to people who made the most significant contribution in the development of free software, as well as socially significant free projects. Commemorative records and letters handed out at the ceremony were mailed to the winners (FSF prize does not imply a monetary reward).

Prize for the promotion and development of free software was Jim Meiring, for GNU Coreutils, which includes utilities such as sort, cat, chmod, chown, chroot, cp, date, dd, echo, hostname, id, ln, ls, etc. Jim is also one of the main

developers of autotools and the creator of Gnulib, who has done a great job of unifying the type code typical for GNU projects.

<https://www.fsf.org/news/lets-encrypt-jim-meyring-and-clarissa-lima-borges-receive-fsfs-2019-free-software-awards>

GEARY 3.36 EMAIL CLIENT RELEASED:

03/15/2020

The Geary 3.36 email client, aimed at the GNOME environment is out. Initially, the project was founded by the Yorba Foundation, which created the popular Shotwell photo manager, but later development went into the hands of the GNOME community. The code is written in Vala and is distributed under the LGPL license.

The goal of the project development is to create a product rich in capabilities, but at the same time extremely easy to use and consuming minimal resources. The mail client is designed both for stand-alone use and for working in conjunction with web-based email

services such as Gmail and Yahoo! Mail. A SQLite database is used to store the message database; a full-text index is created to search the message database. To work with IMAP, a new library based on GObject was used, for working in asynchronous mode.

<https://www.mail-archive.com/gnome-announce-list@gnome.org/msg11638.html>

LINUX KERNEL 5.7 WILL ACCELERATE COMPLEX LIST MATCHING IN NETFILTER

03/16/2020

The developers of the filtering and modification subsystem for Netfilter have published a set of patches that significantly speed up the processing of large nftables, which require checking the combination of subnets, network ports, protocol and MAC addresses. Patches have already been accepted to the nf-next branch, which will be proposed for inclusion in the Linux 5.7 kernel. The most noticeable acceleration was achieved through the use of AVX2 instructions, so far.

Optimizations were introduced into the `nft_set_pipapo` module (Pile PAcKet POlicies), for things like IP and network port ranges (`nft_set_rbtree` and `nft_set_hash` manipulate interval mapping and direct reflection of values). Vectorized with 256-bit AVX2 instructions, the version of `pipapo` on a system with an AMD Epyc 7402 processor, showed a performance increase of 420% when parsing 30 thousand records that included port-protocol bundles. The growth in comparing the bundles from the subnet and the port number when parsing 1000 entries was 87% for IPv4 and 128% for IPv6.

<https://marc.info/?l=netfilter-devel&m=158359998327736&w=2>

THE REDOX OS PROJECT INTRODUCES THE PKGAR PACKAGE MANAGER WRITTEN IN RUST

03/16/2020

As part of this project, a new package format is being developed, a library with package management functions and a

command line tool for creating and extracting a cryptographically verified collection of files. The `pkgar` code is written in Rust and is distributed under the MIT license.

The `pkgar` format does not claim to be universal and is optimized specifically for the Redox operating system. The package manager supports verification of the source by digital signature and integrity control.

<https://github.com/redox-os/pkgar>

POSTFIX 3.5.0 MAIL SERVER RELEASE

03/16/2020

After a year of development, a new stable Postfix mail server branch, 3.5.0, was released. At the same time, they announced the termination of support for the Postfix 3.1 branch, released in early 2016. Postfix is one of the rare projects combining high security, reliability and performance at the same time, which is achieved thanks to a well-thought-out architecture and a rather strict policy for code design and audit of patches. The project

code is distributed under the EPL 2.0 (Eclipse Public license) and IPL 1.0 (IBM Public License) licenses

<https://www.mail-archive.com/postfix-announce@postfix.org/msg00063.html>

SECOND ALPHA RELEASE OF THE DEBIAN 11 BULLSEYE INSTALLER

03/16/2020

The second alpha release of the installer for Debian's next major release, "Bullseye," is available for testing. The final release is expected in mid-2021. We don't usually cover alpha releases, but there seems to be a lot of interest.

<https://lists.debian.org/debian-devel-announce/2020/03/msg00005.html>

NSCDE, CDE-STYLE RETRO ENVIRONMENT WITH STATE-OF-THE-ART TECHNOLOGY:

03/17/2020

The NsCDE (Not so Common Desktop Environment) project, a retro-style CDE interface adapted for use on modern Unix-like systems and Linux is available for download. The environment is based on the FVWM window manager with themes, applications, patches and add-ons to recreate the original CDE desktop. The project code is distributed under the GPLv3 license. Add-ins are written in Python and Shell.

The aim of the project is to provide a comfortable and convenient environment for lovers of retro-styling, supporting modern technology without loss of functionality. To give CDE-style user applications that are being launched, the proper skins, generators for Xt, Xaw, Motif, GTK2, GTK3, Qt4, and Qt5 are available, allowing you to style most applications using X11 with a retro interface. NsCDE allows you to combine CDE design and modern technologies, such as font rasterization using XFT, Unicode, dynamic and functional menus, virtual desktops, applets, desktop wallpapers, themes / icons, etc.

<https://github.com/NsCDE/NsCDE>

FEDORA PLANS TO UPGRADE RPM FROM BERKELEYDB TO SQLITE:

03/17/2020

Fedora Linux developers intend to migrate the RPM package database (rpmdb) from BerkeleyDB to SQLite. The main reason for the rip-and-replace is the use of an unmaintained version of Berkeley DB 5.x in rpmdb, which has not been updated for several years. The reason it has not been upgraded to a newer release is because of a license change in v6.x (RPM is supplied under GPLv2, and AGPL is incompatible with GPLv2). On Fedora 34, BerkeleyDB support will be read-only.

<https://lists.fedoraproject.org/archives/list/devel@lists.fedoraproject.org/thread/YYOEZO2FO2E2T6KO25434EBDTIOWK5OM/>

OPENSILVER PROJECT DEVELOPS OPEN SILVERLIGHT:

03/17/2020

The OpenSilver project is aimed at creating an open implementation of the Silverlight platform. As is the case with Adobe Flash, Silverlight development was halted in favor of the use of standard Web-based technologies. At one time, the open implementation of Silverlight - Moonlight was developed on Mono, but its development was stopped due to the lack of demand for technology by users. (Indeed, why ask why again?)

The OpenSilver project made another attempt to revive Silverlight technology, which allows you to create interactive web-applications using C #, XAML and .NET. One of the main objectives of the project is to extend the life of existing Silverlight-applications in the event of termination of platform support and termination of browser support for plug-ins. However, proponents of .NET technology and C # can also use OpenSilver to create new programs.

<https://opensilver.net/announcements/introducing-opensilver.aspx>

FEDORA 32 BETA:

03/17/2020

Testing of the beta version of the Fedora 32 distribution has begun. The beta release signalled the transition to the final stage of testing, in which only critical errors are allowed. The release is scheduled for late April. The release covers Fedora Workstation, Fedora Server, Fedora Silverblue, and Live cd's. Desktop spins for environments like KDE Plasma 5, Xfce, MATE, Cinnamon, LXDE and LXQt. Builds are available for x86_64, ARM (Raspberry Pi 2 and 3), ARM64 (AArch64) and Power.

<https://fedoramagazine.org/announcing-the-release-of-fedora-32-beta/>

JAVA SE 14 RELEASED:

03/18/2020

After six months of development, Oracle released Java SE 14 (Java Platform, Standard Edition 14), which uses the OpenJDK open source project as its reference implementation. Java SE 14 maintains backward

compatibility with previous releases of the Java platform; all previously written Java projects will work without changes when launched under the new version. Ready-to-install Java SE 14 builds (JDK, JRE, and Server JRE) are available for Linux (x86_64), Windows, and macOS. The Java 14 reference implementation developed as part of the OpenJDK project is fully open under the GPLv2 license with GNU ClassPath exceptions that allow dynamic linking to commercial products.

<http://mail.openjdk.java.net/pipermail/announce/2020-March/000282.htm>



Since Lucas absconded, we cannot fill his slot with more Lucas-stuff, so we went with something I think will be fun and interactive. (Also as I know nothing about rust or go). This may also help some of you who happen to be studying towards OSCP – but I am not saying it will. See: <https://forum.hackthebox.eu/discussion/1730/a-script-kiddie-s-guide-to-passing-oscp-on-your-first-attempt/p1>

Last issue, we did a quick overview of permissions on a Linux system. This issue, we will quickly discuss tools. We need to lay some groundwork first, before going to practical. Tools are handy if you do not want to do every last thing by hand. That said, you still need to know your command-line tools (commands). We already looked at 'id' and 'whoami'. You also need to know 'ifconfig' and 'ip', to see what network interfaces are up. 'Netstat', 'arp' and 'route' (dig?) on those interfaces. Netcat (nc) and 'iptables' at least. You also need to know where Linux keeps its configuration files and what

applications are installed. You need to know which processes are running (ps). There is no shame in keeping a pocket book or .txt-file on a USB thumb drive for reference!

CTF or capture the flag, is an outflow of offsec. It creates a safe haven and an outlet for what you have learned (idle hands and all that jazz...). There are distributions brimming with tools, like Kali or blackArch, but I do not want to tie you to a distribution, or make you a skiddie. There are many blogs around the interwebs that you can follow, when it comes to offsec. Here is one: <https://offsec.vchur.dk/>

They mention an interesting tool, linux enumeration, that is available on github, for your perusal: <https://offsec.vchur.dk/2019/02/26/linux-enum/>

Don't stop there; look at all the tools in that list. LinEnum is also particularly useful. Do yourself a favour and copy all those tools to a

USB thumb drive. They are tiny, so that old 256MB thumb drive you have no use for, just became useful again!

If you look at this enumeration shell script, you will see it is in bash, unlike most other tools written in Python. This has the benefit of working on a system that does not have python installed. (They say, a bad workman blames his tools, so be sure to read through the script! *I did!). This is about a thousand lines of if-statements. As this is a shell script, a thousand lines can run in a second. I am all for learning the command-line, but I am also lazy. Instead of typing the same stuff over and over, script them. This script is also quite recent and being actively developed. With CTF, you are usually given a low level user/password and have to work your way up. With pen testing, you usually gain the shell by some exploit. The difference here is knowing the account you occupy's password...

The other part of the equation;

the machine to be exploited. You can find one at: <https://www.vulnhub.com/> - there are other websites you can find more of these too. I suggest getting a vulnerable Ubuntu or Debian machine, as this is what you know, being a FCM reader. This will boost your confidence and make it easy to start. Like the Hitch-hikers guide says: Don't panic!

I also have to address the elephant in the room. Please use a vulnerable VM and don't try hacking your local .gov website. We are NOT trying to get you into trouble, but knowledge is power. This goes double for those who pester me on Telegram about this.

So what is Linux privilege escalation all about? First, it's collecting. (Enumeration), then processing (analysis), then search & refine, then goto 10. Yes, that is the recipe. However, you need to avoid going down a black hole that sucks up all your time and effort. Plan! It may sound convoluted, but have a plan – before you start. Become Santa. Make a list and

check it twice.

Where would you start? Good question! The 'find' or 'which' command can be your friend. You need to know what you are working with. For example: 'find / -name python*' or 'which python'. So we need to look for cc, gcc, python, perl, at least. Maybe put that at the top of your list and work down. There is no surefire way, so trial and error is perfectly acceptable. See if you can access or read some of the common locations. Always read the user's history file. (history). Look for mounted file systems or unusual ones (df). Etcetera, etcetera. Mundane things, like 'cron', can be a goldmine! Make a list as you go along and refine that list. Check for things like 'curl' and 'wget' and 'nc' that allow you to transfer files, if you do not have what you need.

(Like the bash script above). Your toolbox is the shell itself. SSH is as valid to your PC as it is to that PC. It is advisable to create an archive of your enumeration and send it to an offline PC where you can work on your 'intel' at your own pace. There may be commands you have never used (mknc), that you need to brush up on. As they say, all is fair in love and war. Practice makes perfect?

Now for some online reading:

https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_linux.html

<https://payatu.com/guide-linux-privilege-escalation>

<https://www.sans.org/reading-room/whitepapers/linux/paper/37562>

Yes, you have to read those, it will give you ideas and get you in the right mindset. I am not linking the gotmilk (g0tmi1k) website as it is linked in one of those pages, but go there. Pay attention to the commands being used, you need to know those in your sleep. Notice that advice on (Linux) privilege escalation is not structured. There seems to be no pattern. However, you need to make a recipe that works for you.

Next issue we will look at some practical!

I will give you a lot more links then.

Complaints or comments? Yes, I am a scatterbrain. E-mail us: misc@fullcirclemagazine.org



DistroWatch.com

Put the fun back into computing. Use Linux, BSD.



Erik has been in IT for 30+ years. He has seen technology come and go. From repairing washing machine sized hard drives with multimeters and oscilloscopes, laying cable, to scaling 3G towers, he's done it.



A quick update on the recipe-scrapers library that I wrote about last month. Right now, there are 47 different recipe sites that are now supported, 5 of which I wrote for the project. I have a few more sites that I am working on for the project, so that number will continue to grow. Many of the scrapers are dedicated to non-United States sites in many different languages. I will probably explain the process of creating your own scraper in a future article.

As most of you know, I act as an unofficial support outlet for Page, the GUI designer for Python using Tkinter. On average, I spend probably 5 hours a week answering questions from users, both brand new to Page and users who have been using Page for years. I also help out Don Rozenberg with testing new development builds, trying to break it in as many ways as I can. Once I can't break it anymore, Don usually creates a release. It's a very time consuming job, but one I really enjoy.

Of all the questions I get about using Page, the one I get the most is how to create a program with multiple forms. The answer to this is really pretty easy, but is not as straight-forward as a user would think, hence the questions. The next question is how do I get the forms or windows to communicate with each other. My good friend Halvard from Norway asked how to have one form read information from another in "real time". Again, while the answer is easy, it's not something that most users would try before they ask the question. So, in this edition, I intend to present a very simple demo to help understand the process. AND there's an added benefit in that this solution is not limited to a Page GUI program. It can be used for any Python program including CLI programs. Your imagination is the only limit.

So, I thought I'd throw together a quick demo using Page to show how to deal with both ideas. I'm going to use Page since the process is much easier to show in a GUI, and since the first question is

about dealing with multiple form Page programs.

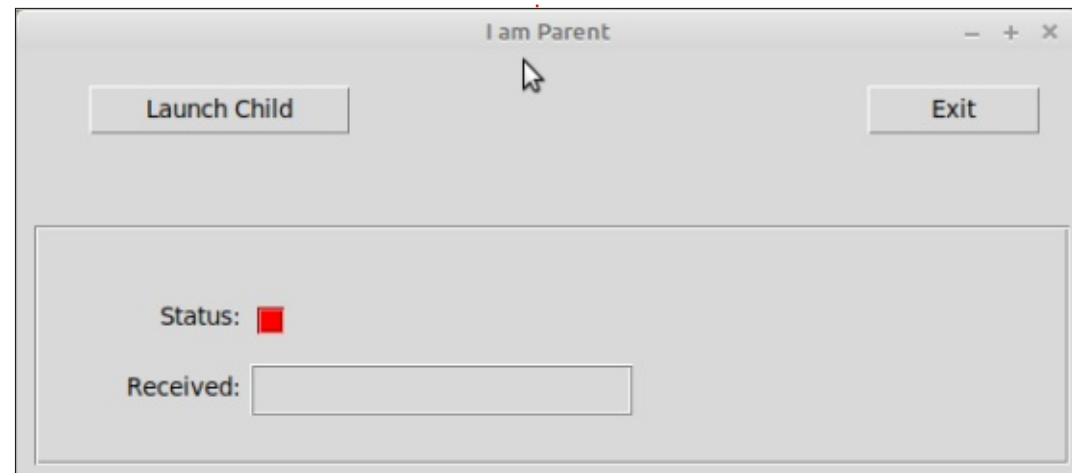
The project will consist of two Page forms, one called "Parent" and the other called "Child". The Parent program will launch the Child program and will receive data from the child.

FORM DESIGN

We'll create the Parent form first. I won't bore you with the form creation details, I'll just provide a screenshot of the form and give you a small amount of important information about some special attributes of some of the widgets.

Below is what the Parent form looks like. I didn't spend much time on making it pretty and mainly kept the attributes for everything on the form to their defaults where possible.

As you can see, it's a very simple form. Two buttons and four labels. The two buttons are named or aliased (from left to right) as btnLaunch and btnExit. There two static labels (status and received) and two dynamic labels, one that is a simple coloured square which shows the connection status to the child form and one (that shows as a fancy ribbed box) which has the textvariable set as DataReceived so it can be updated easily by code.



This will, as the variable suggests, contain the data that comes from the child form. Before I saved the form, I moved it to the middle-left of the screen. The child form will be positioned to the middle-right side of the screen.

btnLaunch has the command attribute set to “on_btnLaunch” and the btnExit has the command attribute set to “on_btnExit”. These are the names of the callback functions for each of the buttons. The only other in the top_level form is the title of “I am Parent”.

Next, we’ll design our child program. This one is a bit more complicated, but not horribly so.



As you can see, there is a small simple keypad similar to a “10 key” with 3 helper buttons, all in a frame. There is also a label that will display the value of the key presses that has the textvariable set to DisplayLabel. The helper buttons are Clear, Bksp (Backspace) and Enter. At this point the enter key does nothing. There is also an Exit button.

The three helper buttons have the command attributes set to on_btnClear, on_btnBackspace and on_btnEnter, which, again, are the callback functions, and the exit button has its command attribute set to on_btnExit.

The 11 keypad buttons don’t use the command attribute set, since it’s easier to set the callback function, which requires a parameter containing which button was clicked, by using the bind command – which we will see in a few minutes. We’ll set the bindings in the _support module.

THE COMMUNICATIONS MAGIC

To communicate between

programs, we use a shared python file, in this case called “shared.py”. Really apropos filename, huh? This module is imported into both (or as many programs as needed) programs as a standard import...

Import shared

The file itself is actually an empty file. There is nothing in it. However, since both of our programs have imported it, they can each read from and write to it.

However, you need to be careful to make sure that before you try to read the value of a variable from it, the value must have already been written to the shared module. We’ll discuss this some more when we examine the code.

THE CODE

The code for the two _support.py modules will be presented below. It’s presented almost in its entirety. The code for the GUI files won’t be presented,

nor will the .tcl files, however the GUI.py files will be available from the pastebin repository so you can actually run the programs.

As always, we’ll start with the imports section for the parent_support.py file. Notice we import child.py, child_support.py, and shared.py

```
import sys
import child
import child_support
import shared
```

The next function (below) is provided by Page for us, which is the set_Tk_var function. This gives us the access to the Label that displays the values that are generated by the child program.

Next up is the init function. This is the very last thing that gets run within the program before the GUI is shown to the user, so we run any initialization and setup tasks from this function. The top part of the function is already written for us by Page. I always provide the comment box, just to give me a

```
def set_Tk_var():
    global DataReceived
    DataReceived = tk.StringVar()
    DataReceived.set('')
```

“landmark” to easily find the function. We’ll discuss my added code below...

The first two lines of my added code, set two variables in the shared module. That way, when the child program starts up, the variables are already there and can be written to when needed. We also use those variables in the next function so they need to be initialized right away. If we don’t, Python will throw an error.

The next thing we do is assign an alias for the status label, which is the red square that shows when the child program is running and connected to the shared module. Finally, I set up a timer function that Tkinter provides called “root.after”. This is an event that

fires every X milliseconds to take care of just about any kind of repetitive task you want to do. You can also create multiple ‘root.after’ timers that run simultaneously. The basic syntax is:

```
handle = root.after(ms, callback)
```

In the case above, the handle is called “comm1” which lets me know that this particular timer is used to communicate with the child process. Notice that I set the time to 0, which means that the callback function will be called immediately, and the final parameter is the name of the callback function.

Bottom right is the callback function code...

```
def init(top, gui, *args, **kwargs):
    global w, top_level, root
    w = gui
    top_level = top
    root = top
    # =====
    # My init code starts...
    # =====
    shared.child_active = False
    shared.ReadyToRead = False
    global LblStat
    LblStat = w.Label15
    LblStat.configure(background='RED')
    global comm1
    comm1 = root.after(0, on_tick)
```

```
def on_btnExit():
    # print('parent_support.on_btnExit')
    # sys.stdout.flush()
    destroy_window()
```

First, we set two global variables, comm1 which is the handle for the timer, and LblStat which is the alias for our little red square. Next, we access the shared module to see if the child process is running by checking shared.child_active to see if it’s True. This is set as soon as the child program starts up. If it is, we set the square colored label to “Green” to show that the child process is running and then we check to see if shared.ReadyToRead is set to True – which is basically a flag that says that one of the numeric keys has been clicked. If it is, we get that data, put it into the display label with the .set() method, and clear the ReadyToRead flag, so we can wait for the next click event on the child process. If the shared.child_active flag is False, we

reset the coloured square to Red. This way, when the child program is exited, we will know it visually.

Finally, we “re-arm” the timer routine, this time to check 100 ms from that point.

Now, we look at the on_btnExit callback function (shown above). It’s very simple. We simply call the destroy_window() function that will cleanly end the program. The destroy_window function is provided by Page as is the on_btnExit callback skeleton, since we added the callback name in the command attribute for the exit button. All we have to do is add the line “destroy_window()”.

Next, we’ll look at the

```
def on_tick():
    global comm1, LblStat
    if shared.child_active == True:
        LblStat.configure(background='GREEN')
        if shared.ReadyToRead:
            DataReceived.set(shared.ChildData)
            shared.ReadyToRead = False
    elif shared.child_active == False:
        LblStat.configure(background='RED')
    comm1 = root.after(100, on_tick)
```

```
def on_btnLaunch():  
    # print('parent_support.on_btnLaunch')  
    # sys.stdout.flush()  
    child.create_Toplevel1(root)
```

btnLaunch callback function (above). This is how we make the child program start. Again, we used the command attribute for the button in Page, so the skeleton is started for us...

The only line we need to enter here is the last one. Since we have already imported the child.py GUI file at the top of the code, we just need to call the create_Toplevel1() function. This is the entry point for the program when it is called from another program.

Finally, I've provided the destroy_window() (below) which is provided by Page, just so you can see it.

Now we'll look at the child program. It is a bit more complicated, but not overly so. Again, I'm going to provide the code here for only the child_support.py module.

```
def destroy_window():  
    # Function which closes the window.  
    global top_level  
    top_level.destroy()  
    top_level = None
```

Again, we'll start with the import section. Notice here, that we need to import only the shared module, since we don't need to call any functions from the parent.

```
import sys  
import shared
```

Top right is the definition for the label that shows the running value from the keypad button entries.

The first thing we do is set up a global variable to hold the accumulated value of the keypad entries. We then call the function setup_bindings() that attaches the callback function to all of the buttons of the keypad. Finally, we set the shared.child_active flag to True.

Since we are going to pass parameters to the callback for the

```
def set_Tk_var():  
    global DisplayLabel  
    DisplayLabel = tk.StringVar()  
    DisplayLabel.set('Label')
```

Here is the init function from the child program. Again, you can see where my code starts.

```
def init(top, gui, *args, **kwargs):  
    global w, top_level, root  
    w = gui  
    top_level = top  
    root = top  
    # =====  
    # My init code starts...  
    # =====  
    global valu  
    valu = ''  
    setup_bindings()  
    shared.child_active = True
```

keypad buttons, it's much easier to deal with things here (below) than to try to do it within Page through the command attribute.

Now we define the callback routine code (next page, top left)

```
def setup_bindings():  
    w.btn0.bind('<Button-1>', lambda e: on_btnClick(e, 0))  
    w.btn1.bind('<Button-1>', lambda e: on_btnClick(e, 1))  
    w.btn2.bind('<Button-1>', lambda e: on_btnClick(e, 2))  
    w.btn3.bind('<Button-1>', lambda e: on_btnClick(e, 3))  
    w.btn4.bind('<Button-1>', lambda e: on_btnClick(e, 4))  
    w.btn5.bind('<Button-1>', lambda e: on_btnClick(e, 5))  
    w.btn6.bind('<Button-1>', lambda e: on_btnClick(e, 6))  
    w.btn7.bind('<Button-1>', lambda e: on_btnClick(e, 7))  
    w.btn8.bind('<Button-1>', lambda e: on_btnClick(e, 8))  
    w.btn9.bind('<Button-1>', lambda e: on_btnClick(e, 9))  
    w.btnDot.bind('<Button-1>', lambda e: on_btnClick(e,  
10))
```

for when a keypad button is clicked. Notice this must be done from scratch, since Page has no idea of the need for the function.

In the callback, we simply take the value (which is the number of


```
def on_btnClick(e, which):
    global valu
    if which < 10:
        valu = valu + str(which)
    elif which == 10:
        valu = valu + "."
    shared.ChildData = valu
    DisplayLabel.set(valu)
    shared.ReadyToRead = True
```

the button) and append it, as a string, to the valu variable. We also check to see if the period key (value 10) was pressed, and if it was, then we add the period into the display value. Finally, we put the data into the DisplayLabel through the .set() method, and set shared.ReadyToRead to True, so the parent knows to pull the data.

We don't do anything with the Enter button, so we just leave the skeleton for later use (far right).

As usual,, I've put the code for the programs on Pastebin. You can find the links below:

parent.py -
<https://pastebin.com/AZXXvuAU>

parent_support.py -
<https://pastebin.com/3iBHqCNO>

child.py -
<https://pastebin.com/bwZLnkHc>

child_support.py -
<https://pastebin.com/Vg0K1w5G>

I hope this article has given you some food for thought that can be used in your own programming.

Until next time, keep coding.



Greg Walters is a retired programmer living in Central Texas, USA. He has been a programmer since 1972 and in his spare time, he is an author, amateur photographer, luthier, fair musician and a pretty darn good cook. He still is the owner of RainyDaySolutions a consulting company and he spends most of his time writing articles for FCM and tutorials. His website is www.thedesignatedgeek.xyz.

```
def on_btnEnter():
    print('child_support.on_btnEnter')
    sys.stdout.flush()
```

The callback for the Exit button is mostly the same as for the parent, but we also set shared.child_active to False, so the Parent knows to change the status square from Green to Red and not to try to poll.

```
def on_btnExit():
    print('child_support.on_btnExit')
    sys.stdout.flush()
    shared.child_active = False
    destroy_window()
```

The btnClear callback function sets the global valu to an empty string, sets data into the shared module and the display label, and then sets the shared.ReadyToRead flag to True.

```
def on_btnClear():
    # print('child_support.on_btnClear')
    # sys.stdout.flush()
    global valu
    valu = ''
    shared.ChildData = valu
    DisplayLabel.set(valu)
    shared.ReadyToRead = True
```

Finally, we deal with the callback for the Backspace button. We simply strip the last character from the valu string, display it, pass it to the shared module, and set the flag so that the parent program will read it.

```
def on_btnBackspace():
    # print('child_support.on_btnBackspace')
    # sys.stdout.flush()
    global valu
    valu = valu[:len(valu)-1]
    shared.ChildData = valu
    DisplayLabel.set(valu)
    shared.ReadyToRead = True
```



HOW-TO

Written by Erik

Ubuntu And Security

One of our readers, Joe Wong, wanted to know how to set up things like TOR and nmap and the like on Ubuntu. As his questions were too broad to cover in questions and answers, I decided to do a mini tutorial on it.

Let us start with the short ones, and work ourselves up to the longer winded ones? Nmap is easy. 'Sudo apt install nmap' will do the trick. Should you prefer the GUI, you need to install Zenmap. The nmap website has great tutorials on how to use nmap / zenmap. Documentation here: <https://nmap.org/book/man.html> - I find nmap to be faster and more accurate than angry IP scanner for Linux. There is even a book dedicated to this useful tool. You can read some of it here: <https://nmap.org/book/toc.html>

Similarly, wireshark is available from your repositories, so 'sudo apt install wireshark' will fetch it for you, alternatively search in the software centre. If you need a quick primer,

<https://www.youtube.com/watch?v=TkCSr30UojM> - is a handy link. As network traffic analysers go, this is awesome. If you just want the basic commands, go here: <https://www.tecmint.com/wireshark-network-traffic-analyzer-for-linux/>

TOR comes in two parts, the TOR network, and the TOR browser. The browser installation is as simple as downloading the .deb-file from the TOR browser website and installing it. The other option is to download the .tar-file and extract it to your home folder. The compressed file includes a launcher you can copy to your desktop, if you like. It is a good idea to keep the folder separate from your current Firefox installation. The browser manual is here: <https://tb-manual.torproject.org>

TOR network needs a bit more. It is safest to install TOR from the official repository. To add it, simply edit your sources file. I will use nano here, but the editor does not matter

```
sudo nano
/etc/apt/sources.list.d/tor.list
```

Add the following lines, replacing "bionic" with your version's code-name:

```
deb
https://deb.torproject.org/torproject.org bionic main, and
deb-src
https://deb.torproject.org/torproject.org bionic main
```

You will also need to add the key:

```
curl
https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc
| sudo gpg --import
```

```
gpg --export
A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key
add
```

NOTE: There are double dashes before import and export, word processors do weird things with double dashes.

After the obligatory:

```
sudo apt-get update
```

just type the following

```
sudo apt-get install tor
deb.torproject.org-keyring
torbrowser-launcher
```

Rootkit Hunter :

<http://rkhunter.sourceforge.net/> is not difficult to install and run either. Type:

```
sudo apt install rkhunter
```

There is a bit of an ncurses based setup to go through, but it is really straightforward.

Once installed, rootkit hunter needs you to edit the configuration file a bit:

```
sudo nano /etc/rkhunter.conf
```

and make sure MIRRORS_MODE=0 and WEB_CMD=""

That's it.

Now we get to talk about one of my favourite security tools, Lynis. So many checks, so little time. You can find it here: <https://cisofy.com/lynis/>



HOWTO - UBUNTU AND SECURITY

You can download the compressed file and do it all manually, but it is easier from the terminal. Let us grab the key first:

```
sudo wget -O - https://packages.cisofy.com/keys/cisofy-software-public.key | sudo apt-key add'
```

Now:

```
sudo apt install apt-transport-https
```

Followed by:

```
echo 'Acquire::Languages "none";' | sudo tee /etc/apt/apt.conf.d/99disable-translations'
```

IF YOU ARE USING IT IN ENGLISH.

Now add the sources:

```
echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list
```

You know the drill after this:

```
sudo apt update && sudo apt install lynis
```

Lynis is currently at 2.7.5, but you can install as far back as 2.6.6 for Ubuntu 14.04.

Lynis is a tool that needs to be run as root or else it will just skip some of the most important tests:

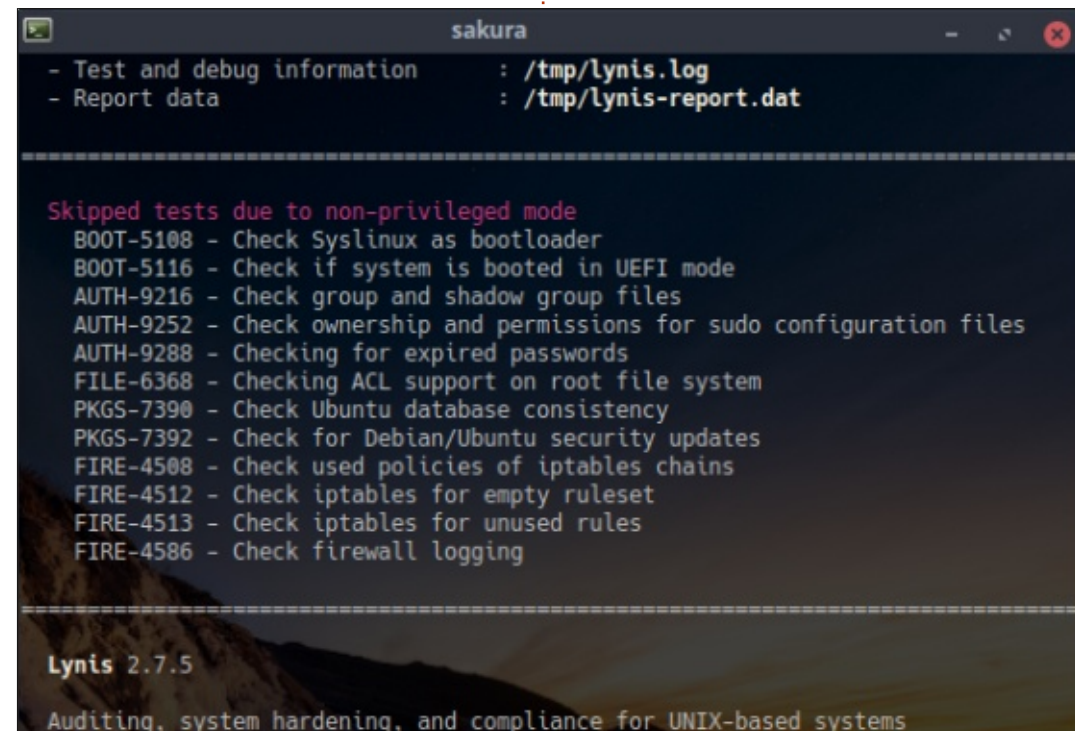
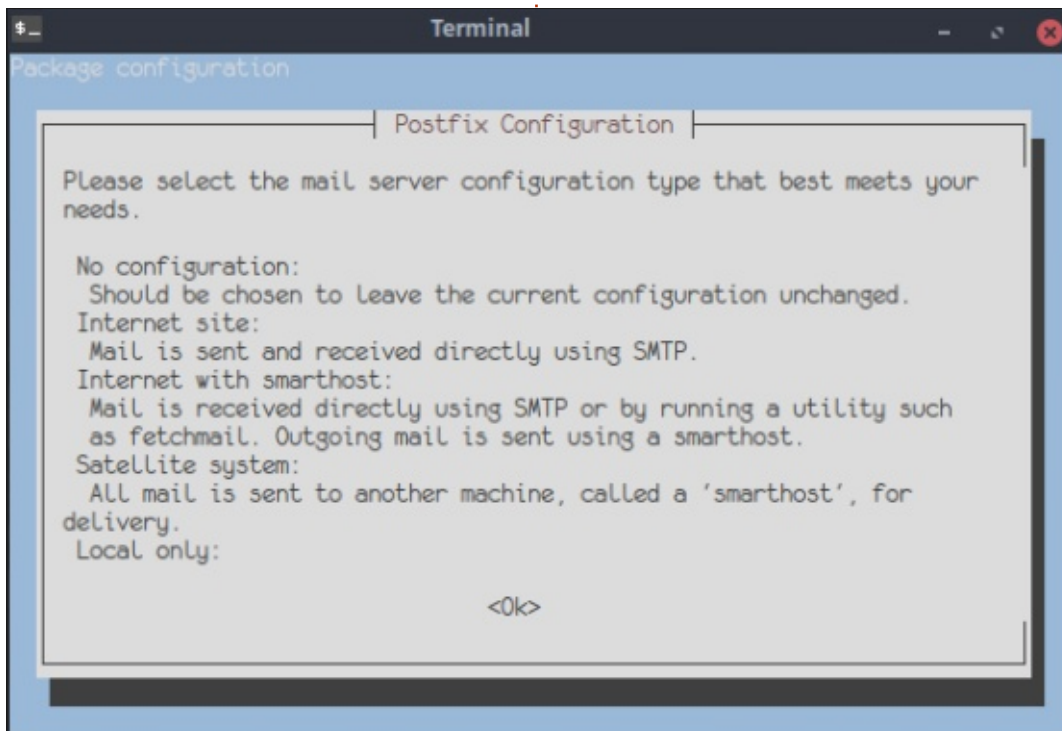
```
sudo lynis audit system
```

REFERENCES:

<https://packages.cisofy.com/community/#debian-ubuntu>

There are other ways to install Lynis, but this is the easiest.

If there are any queries on the installation of these tools, or maybe their use, please email us on misc@fullcirclemagazine.org





HOW-TO

Written by Erik

Website:

<https://rawtherapee.com/>

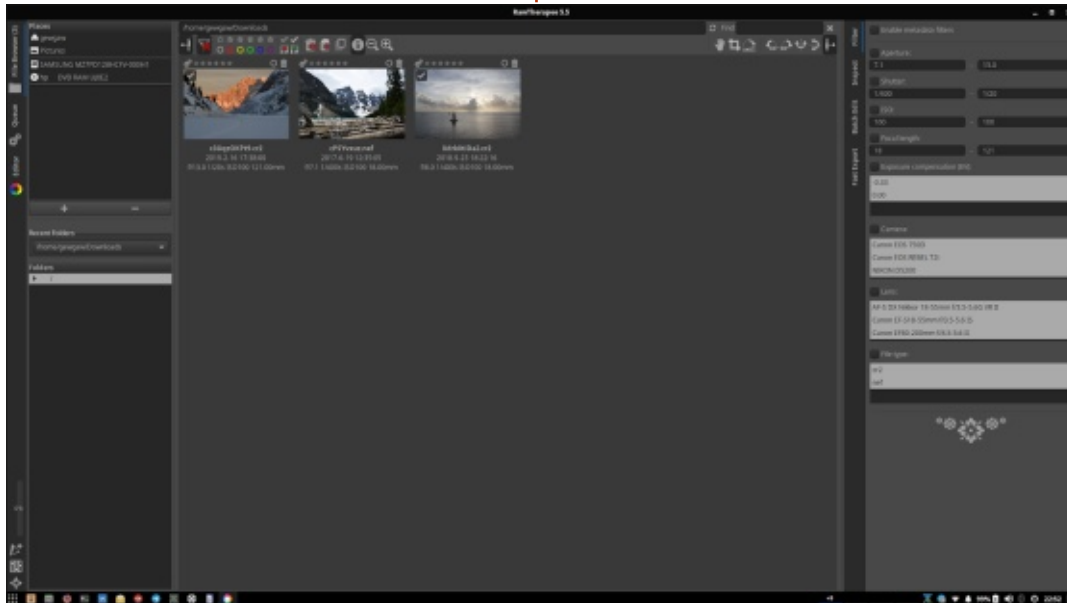
Version 5.6

Price: Free!

We have been looking at Darktable in FCM, but know it is not your only choice in photo editing. Today we look at another excellent piece of open source software. It may seem a bit daunting when you open it at first. I know I was lost the first time I opened this.

Left to right, we have five panes, the first being the itty-bitty

strip, with your file browser queue. Then browser, main window, another strip, and editor. (In editor mode, we only have four panes). We will be spending our time in the editor. Your keen eye may have spotted that there are little bars with an arrow attached in the menu bars. These are the show / hide buttons. Mouse over may say "i", "shift-i" and "alt-i", but the keyboard shortcuts work only once you have clicked these buttons (but not the very first time). This will give you a large canvas to work on. Now that you have hidden all the confusing looking panels,



Rawtherapee - Pt1

you will find that it is actually pretty intuitive. Mouse wheel, or plus and minus, will zoom. Crop is 'c', straighten is 's', and so forth. The very last pane on the right is not a static pane, you will see it actually change as you select different tools. Open the pane, look at it, and press 's'. The little blue underline bar moved from the first icon to the fifth, and changed the panel below it. This is what I mean when I say it is not static.

Your homework is to mouse over the different icons and see what they do.

The image we will be playing with today (shown below) is: <https://www.wesaturate.com/photo/Xdrk0tiDa2>

Please grab the RAW image. The JPEG is this pink processed image.

Once you have opened the



picture in Rawtherapee, I need you to open the very right-hand pane again. This is where we will be working. We will start with exposure. You will see that the layout has workflow in mind. To demonstrate how this great application works, we will edit this basic picture. Look at the tone curve. Rawtherapee has already done the heavy lifting for you. However, it may not be to your liking. What I am about to show you is for you to learn post processing. It is not the “best” way, as best is subjective. As long as YOU like it - and maybe your mother – unless you are doing post processing on your pictures for other people, on instagram or facebook, where you are conditioned Pavlov’s dog-style, for likes.

Let’s start with black-and-white. There is a reason there are two triangles with exclamation marks in the top bar. Think of them as ‘clipping’ black and white. You will see eight points marked on your histogram, if you are using the above picture. Too many, I think for a simple image like this. You can remove some by clicking and holding and dragging the point to the very bottom. They should turn

red as you mouse-over them, then, as you drag them off the bottom, the line should snap back. Should you make any mistakes, just click “auto matched tone curve” and it should be reset. From the left, I want you to remove the second and third dot or pin. Also I want you to remove the second-last pin. Your histogram should have only five pins. The image has almost no black, so we can drag the leftmost pin until where our histogram starts rising. Keep an eye on your picture whilst doing this. This should cause the shadow of the yacht to become more pronounced. Bring your rightmost pin a block in also, to help with the bright white in the sky. Now click



the two triangles with exclamation points in them in the menu. YUK! you may say. Relax, this is showing you where pure white and pure black exist within your picture, It does not change anything. You can turn them off now.

Let me talk about the three sliders above your histogram. Lightness, contrast and saturation are all well and good, but Rawtherapee supports L.a.b. colours as well. In L.a.b., the Luminance can change contrast without saturation. This is important when you need to change the lighting, but keep the saturation the same. If you turn up the contrast to about 35-40, you

will see the water come alive, yet the yacht will become a black blob, which is not ideal. The opposite happens when you turn the contrast down, the life seems to drain from your picture. Contrast in a photo is very important. This gives life and depth to an otherwise mundane picture. I know that sounds weird, but it is true. If you just want to copy what the guy did in the picture above, turn the contrast up full, then go to the white balance icon and drag the red/blue slider all the way to red, and you are done.

Back to editing our borrowed photo. The very first slider is “Exposure compensation”. This tool is very sensitive, so use it sparingly. I use the “+” and “-” buttons to adjust mine. Since this picture is into the light, I want to bring mine down, just a little. Enough to keep the detail in the sky. Again, keep your eye on your histogram, as it will move the histogram towards your leftmost cutoff point. Mine is at “-0.20”. I am going to adjust my saturation to about “35” just to make the sun behind the clouds come alive.

You may think Rawtherapee is a simple editing program. You would

HOWTO - RAWTHERAPEE

be wrong. Keep your mouse in the right-hand pane and scroll your mouse wheel. Lots more adjustments appear. When you have scrolled to the bottom, you should see "Graduated filter". Please click on the crosshairs in the very left-top corner of 'graduated filter'. You should see large crosshairs appear on your photo. Adjust it so that the bottom one aligns with your yacht. Now, next to the word "Graduated filter", you

will see a circle. Click on it. This will turn the filter on. Notice how the sky darkens, but the water stays the same. You are going to want to rotate this so that the light and dark patches match the angle the sun is shining over the clouds. This helps your brain make sense of the photo, that it does not seem "shopped" - Remember, less is more!

I want you to play with the

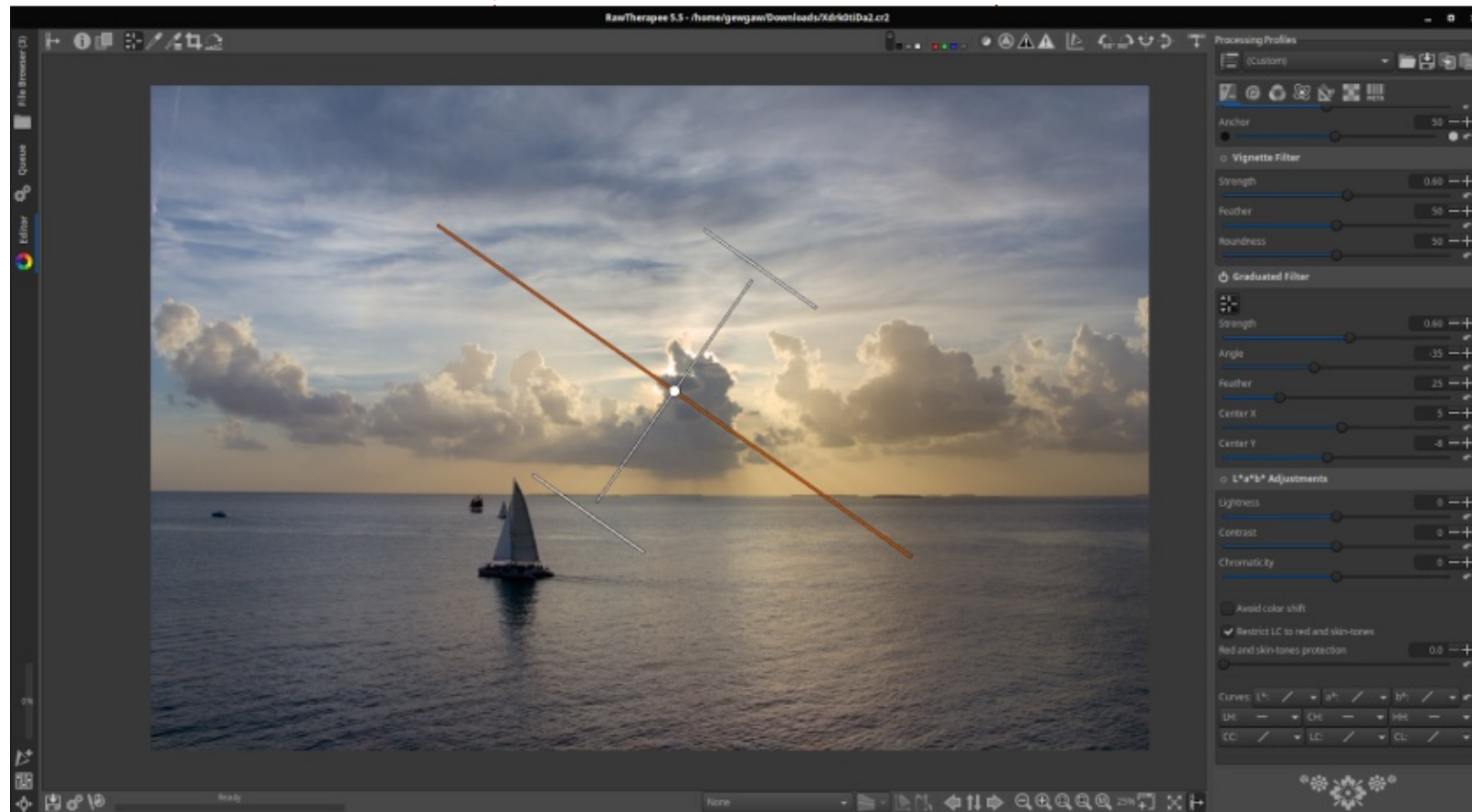
"Strength" slider. Understand where the light and dark are. Next I want you to increase and decrease the "Feather". This is the transition distance between the light and dark.

To get that vintage camera feel, just turn on "Vignette Filter", you do not have to adjust anything. For our use case here, I am going to leave it off. If you scroll your mouse up just a little bit, you will

see "Tone Mapping". Turn this on for instant sharpening. There is, of course, a "Sharpening" section too, but more next month as we explore this excellent application. Party on Wayne, party on Garth.

If you would like more on Rawtherapee, please email us on misc@fullcirclemagazine.org and let us know.

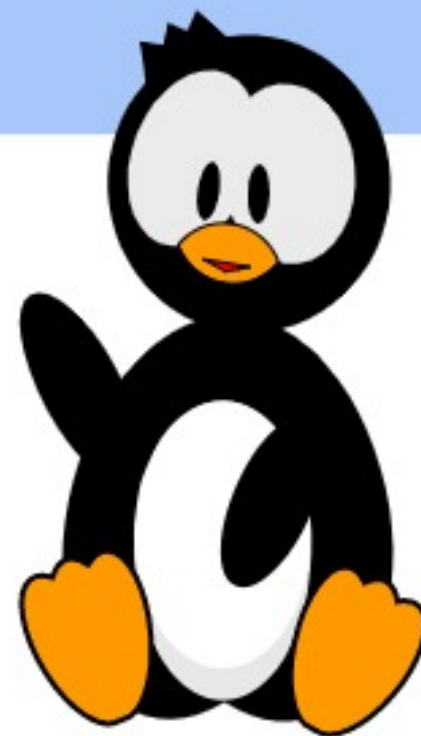
Disclaimer: In no way am I an expert in photo manipulation, I just know a guy who had a dog that gave me some fleas. I thought I may help you scratch an itch also.



The Daily Waddle

**Microsoft is creating
a browser based on
Chrome to replace
Internet Explorer...**

**Good, now we can
download FireFox
even faster!**





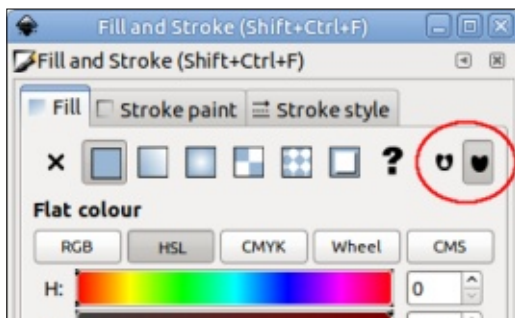
HOW-TO

Written by Mark Crutch

Inkscape - Part 95

This month and next, I'm going to cover a couple of Inkscape features that have fallen through the gaps in my previous coverage. The first of these, disgracefully, dates back to the 4th instalment of this series, way back in 2012! In FCM#64, when describing the options in the Fill and Stroke dialog, I wrote: *"Also being put off for later articles are the Unset Paint button that looks like a question mark, and the two splodges on the right of the Fill tab."*

The Unset Paint button was eventually described in part 30 (FCM issue #90), when I covered its use with clones. But what of the "two splodges on the right of the Fill tab"? For clarity, let's first take a look at a screenshot of the Fill and Stroke dialog, in which I've circled the splodges.



To understand what effect these splodges – which are actually a pair of mutually exclusive radio buttons – have on your objects, we'll need a path to test with. Not just any path will do, however. These buttons have an effect only on paths that are either self-intersecting, or which contain sub-paths. Let's deal with the former to start with: what exactly do I mean by 'self-intersecting'?

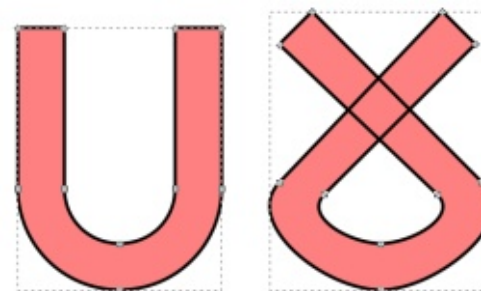
Consider the paths below. The one on the left is just a simple U-shaped filled path. Nothing special, no sneaky tricks. Just 10 nodes forming a shape with a couple of arms. The shape on the right is just a duplicate of the first one, with the end of the left arm moved to the right, and the end of the right arm moved to the left, so the arms cross each other. No nodes were added or removed, they were just



moved around a little.

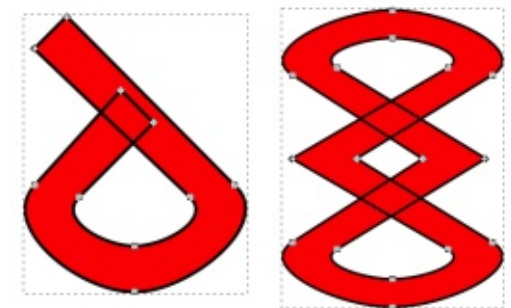
The second shape is a self-intersecting path. It's a closed path that is drawn such that it crosses itself, although the word 'crosses' carries a misleading implication in this case. Remember that Inkscape is a 2D drawing program, with no notion of the third dimension. So when making this shape I didn't really move one arm 'over' the other, as you would do when making the same shape with a piece of string. Rather I moved it 'through' the other, in the same 2D plane. Neither arm is on top of the other. Neither arm 'crosses' the other. Instead the resultant shape simply intersects with itself.

Turning on the stroke and reducing the fill opacity makes this a little clearer:



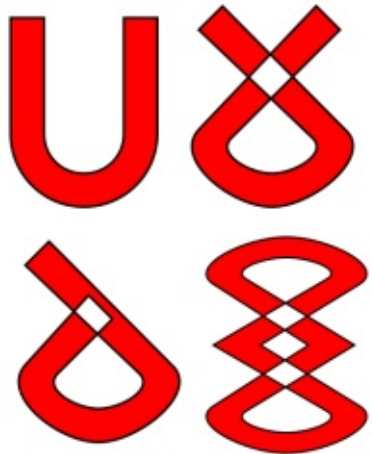
Notice how the stroke is visible for both arms. If one crossed over the other you might expect the stroke of the arm on the bottom to be obscured by the one that's on top, but that's not how things work in the 2D graphics world. You'd also expect the colour of the fill to be a little darker where the two translucent arms cross over, but that's not the case either.

It's also important to note that the arms don't have to completely pass through each other in order to be a self-intersecting shape, and that the shape could self-intersect multiple times, as demonstrated in these variations on the theme:



Now we're all clear on what a self-intersecting path actually is, let's look at how they're affected

by the splodgy radio buttons. The first thing to note is that the images so far have all been taken with the second button selected – the one that’s completely filled in. Switch to the first button, and we get this:



The basic U-shaped path remains unaffected. It’s not a self-intersecting path, and it doesn’t contain any sub-paths, so the radio buttons have no effect. All the others, however, have no fill rendered in the intersecting parts. The stroke is still drawn, but the fill isn’t.

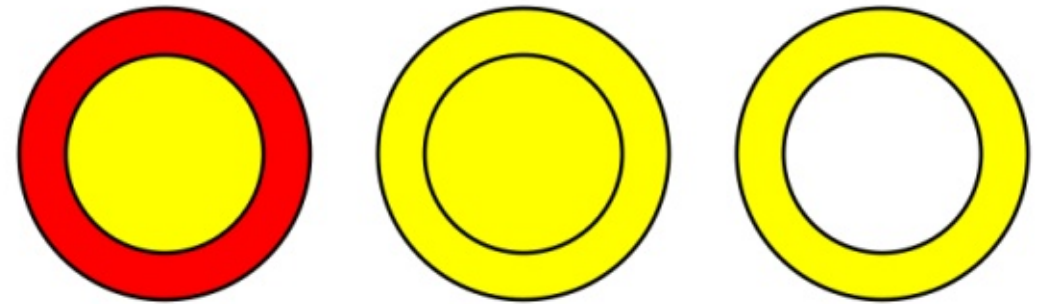
This behaviour is a little confusing at first. Surely the intersecting parts are inside the shape, so they should still be filled, right? Unfortunately our intuitive

idea of in-and-out doesn’t always apply in the world of computer graphics. Instead there are different rules or heuristics for determining whether a point is inside or outside a shape – and the splodgy buttons are used to switch between a couple of those rules. Let’s take a look at paths with sub-paths to try to explain why there’s a need for this choice.

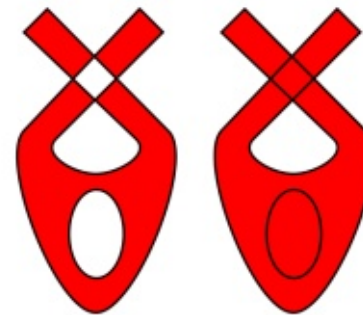
When you look at the self-intersecting shapes above, it’s pretty obvious that the fully-filled option (second button) is the right choice most of the time. Imagine trying to draw a figure-of-eight, only to find that the part where the shape crosses itself is unfilled. Definitely better to use the second option, so we’ll ensure that’s selected. Now we’re going to draw a circle with a hole in it. There are a few ways to achieve this but, to make a point, I’m going to use a very specific method:

- Draw a circle for the outside.
- Draw a smaller circle for the inside.
- Path > Combine to create a complex path, made up of two sub-paths.

In this image (above) you can see the two separate shapes on



the left, and the result of combining them in the middle. The ‘hole’ in the shape is filled – not really what we were after. Switching to the first button, however, gives the expected result, as shown in the version on the right.



Now we’ve got a simple rule-of-thumb: use the left-hand button for paths with sub-paths, and the right-hand button for self-intersecting paths. But what if we have a path that is both self-intersecting and has a sub-path describing a cut-out? Something like this odd piece of jewelry or alien symbol, shown as it appears

with each of the two splodgy radio buttons selected:

On the left we have the problem of no fill in the self-intersecting part, but the hole is fine. With the right-hand button we get a fill in the self-intersecting part, but no hole. Is there any way we can have the best of both options?

The answer is obviously ‘yes’, but to get there it helps to understand what the two heuristics are that we’ve been switching between. The first button has a tooltip that reads “any path self-intersections or subpaths create holes in the fill”, and is referred to as the “even-odd” rule. The heuristic for this is pretty simple:

- Pick a point in the shape.
- Draw an imaginary straight line from that point out of the shape in any direction.

HOWTO - INKSCAPE

- Keep a 'crossing' count, which starts at zero.
- Add one to the count each time the line crosses a path or sub-path boundary.
- If the final count is even, the point was outside the shape. If the count is odd, the point was inside the shape.

By performing this for a point in each region of the shape, Inkscape can determine which areas are inside, and therefore need to be filled, and which are outside. But it does result in self-intersections being counted as outside, and left unfilled.

The second button has a tooltip that reads "fill is solid unless a subpath is counterdirectional", and is referred to as the "non-zero" or "winding" rule. This heuristic relies on the fact that each sub-path has a direction associated with it, and works like this:

- Pick a point in the shape.
- Draw an imaginary straight line from that point out of the shape in any direction.
- Keep a 'winding count' which starts at zero.
- Each time the line crosses a path or sub-path, add one to the count if the path is crossing the line from

left to right (clockwise from the perspective of the point) or subtract one if the path is crossing from right to left (counter-clockwise).

- If the final count is zero the point is outside the shape, otherwise it is inside.

From this algorithm and the mention of "counterdirectional" in the tooltip – you may have already worked out that using the second splodgy button (non-zero) lets us switch sub-paths between filled and unfilled by reversing the direction of the nodes. Fortunately for us, Inkscape makes this fairly easy:

- Select the composite path and switch to the node tool (F2).
- Select a node in the sub-path.
- Use Path > Reverse to reverse the order of the nodes in the sub-path without changing the shape.

You can see the effect of this approach in the following image. In this case I've also added arrow markers to the paths, to clarify what's happening. The first image is our starting path, created by combining an oval with a self-intersecting shape. You can see from the arrows that the sub-path is running counter-clockwise. In the

second image I've reversed the direction of the sub-path, the arrows point the opposite way, and the shape has a hole for the sub-path but not for the self-intersection.



Unfortunately this simple approach doesn't appear to work in the beta of Inkscape v1.0, where the Path > Reverse operation reverses the entire path rather than the selected sub-path. The only option in this case is to use Path > Break Apart to split the shape down into its constituent parts, then use Path > Reverse on just one of those paths, then finally use Path > Combine to recombine them back into your original complex path. This is a definite step backwards in the workflow, so I will be filing a bug about this on the Inkscape issue tracker.

This path-reversing approach

works for simple shapes where the nesting of sub-paths isn't very deep. For more complex arrangements you may need to reverse more than one path to get the effect you want. And if there are also intersections between sub-paths, or self-intersections within them, you may never be able to get just the fill you want, no matter what you try. In those cases you may find it easiest to use the first splodge (even-odd) to fill the entire shape, then create your complex hole arrangement by clipping with a suitably constructed path.

It's worth noting that you might never experience this problem. Punching a hole through a shape is more commonly done using Path > Difference than Path > Combine, and the former usually results in a sub-path going in the right direction. But it's worth knowing about these splodgy buttons and how to work with them, just in case you ever find yourself presented with a path that contains inexplicable holes or fills where it shouldn't.



HOW-TO

Written by Alan Ward

Krita To Rework Old Photos Pt.5

This series is aimed at learning to make something of the old photos in my possession, and of others in the public domain due to their age. You, the reader, are welcome to tag along and, I hope, glean some small insight and perhaps an idea or two from time to time. No promises are made as to the quality of the content, or potential errors and omissions. I am a computer scientist, not a true artist or a professional of image restoration. So please take all this as a best effort, but with no firm guarantees — much as is the case of most open-source software.

In the previous part of this series, we finished up colorizing an 19th century black-and-white landscape view of the castle of Foix in Southern France. For today's part, we will change subjects. We work on an early 20th century image, a studio portrait. Paul Trappen, presented as the world's Strongest Man, was photographed, and the resulting prints sold as a postcard. The result is now available on Wikimedia Commons at address

https://commons.wikimedia.org/wiki/File:Portrait_of_Paul_Trappen.jpg.

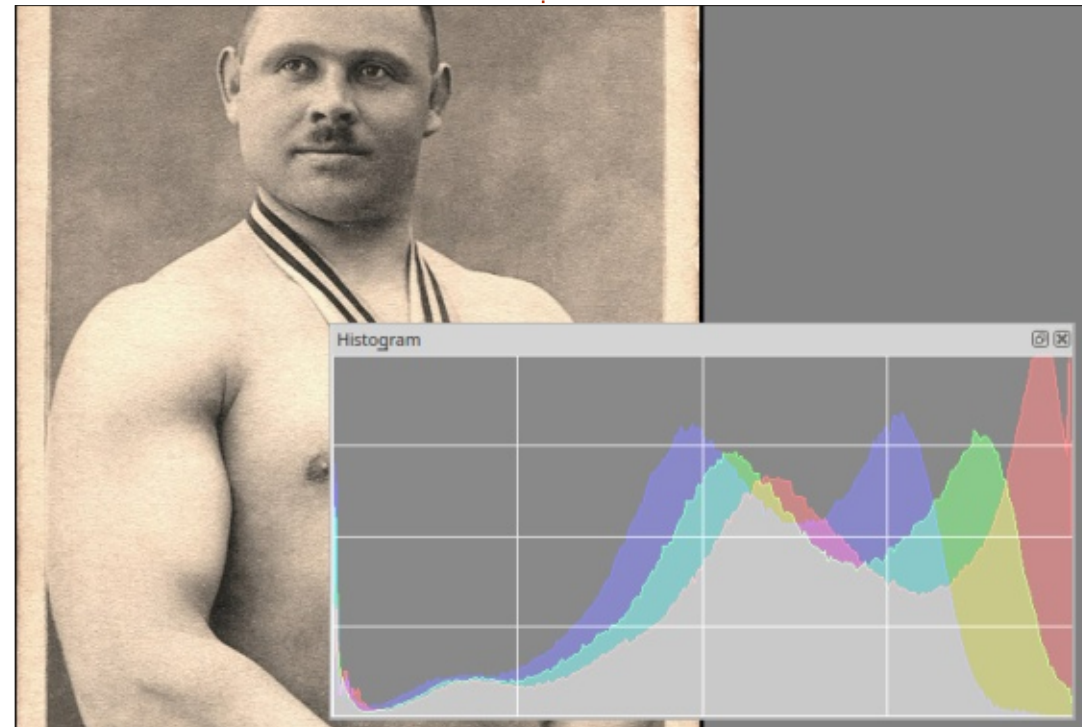


This image shows us some typical traits of an early 20th century studio portrait. Photographic technique had been rather perfected at the time, and subjects were usually presented in a more-or-less contrived --but lifelike-- pose, in front of a suitable

background. The use of large surface-area glass plate negatives allowed fine details to show up well. Lighting tends to be good in most cases, with a wide range of shades of gray that fill in volumes nicely. This is clearly the case in today's exhibit, where the sheer mass of the subject's arms were of interest. However, some areas of his anatomy --the upper chest and arms-- did get washed out a tad by excessive lighting, while the lower face and underarm areas suffer

from a slight lack of light.

All in all, we have a rather good base from which to start. Once opened in Krita, an initial assessment with a histogram confirms our impression of a globally balanced image, though with some preponderance of lighter pixels. Darker shades are merely represented by the subject's briefs. The command in previous versions of Krita to show a histogram used to be at menu

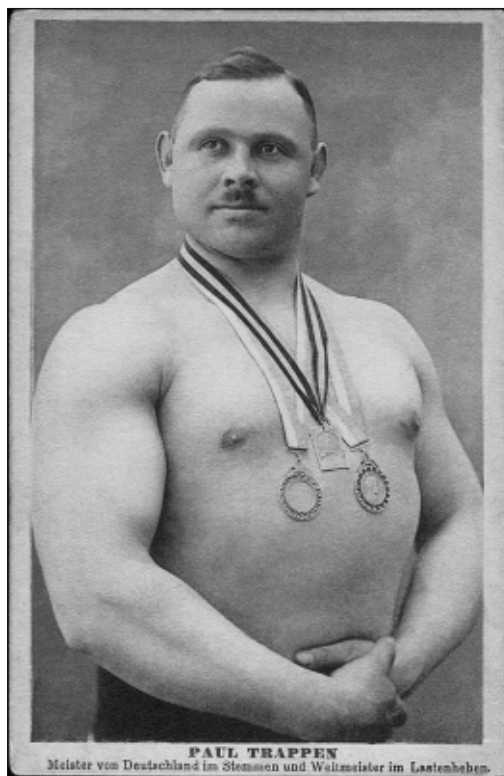


option "Layer", then "Histogram", then "GRAY/Alpha 32 float". In newer versions such as Krita 4.2, however, it seems to have migrated as a separated dockable window ("docker"), that can be invoked from menu option "Settings", then "Dockers", then activate the "Histogram" checkbox:

Three superimposed curves representing the red, green and blue components of the image show us the darker colors (in the left-most quarter of the histogram) are slightly lacking, while frequencies rise as we progress towards the right and the lighter shades of each color. This presentation with individual colors separated makes us aware that there is some imbalance between channels, with more yellow and a touch of extra red towards the extreme right. This is easily seen in the original image, with its sepia (reddish-brown) tinge.

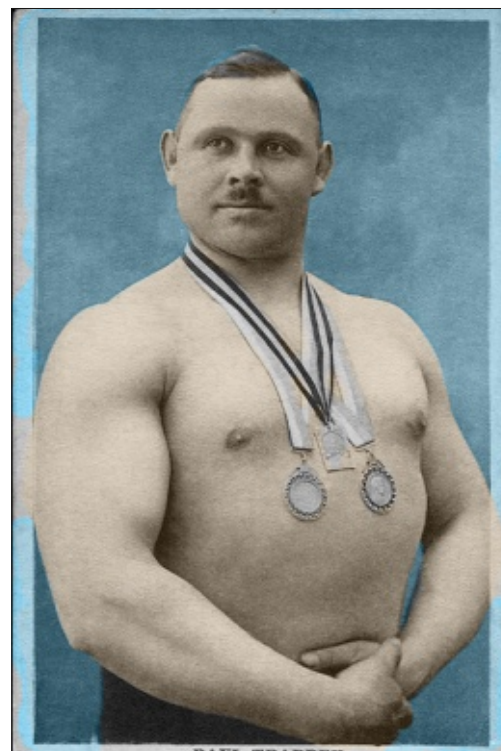
This is the first alteration we will need to make, to obtain a truly neutral base on which to start working. To reduce the colors in an image, in Krita there is a handy tool called "desaturation": select menu option "Filter", "Adjust", then "Desaturate". Then try out

different options to see which calculation method suits your image best. In this case, I gave the athlete the "Min" setting, which conserves the lowest (darkest) values while soothing somewhat the (slightly) overexposed areas of skin.



I then created a new layer, converted its use from "Normal" to "Color", and then painted in some basic skin color. This technique of merely superimposing a new layer instead of altering the original has its uses, which will become

apparent later on. For the background, since we cannot really know what tone backdrop the original studio used, we can only make a reasonable supposition. I went for a rather neutral blue, since that would have given the subject an impression of sky -- even though he would have known full well that the exact color would not appear in the photograph.



Just these two simple tweaks already give a more lifelike impression than the original. However, we do need to get these first main colors just right. Also, be

careful on the boundaries between these colors. Other color limits are not important just yet, since we will need to paint in further colors for details.

But, precisely which colors do we need to use? Without any supplementary information on the subject, we are incapable of knowing what was the color of his hair or eyes, what colors were used for the ribbons of the medals, or even what metal these were made of. With a bit of creative imagination, and keeping to the domain of reason as closely as

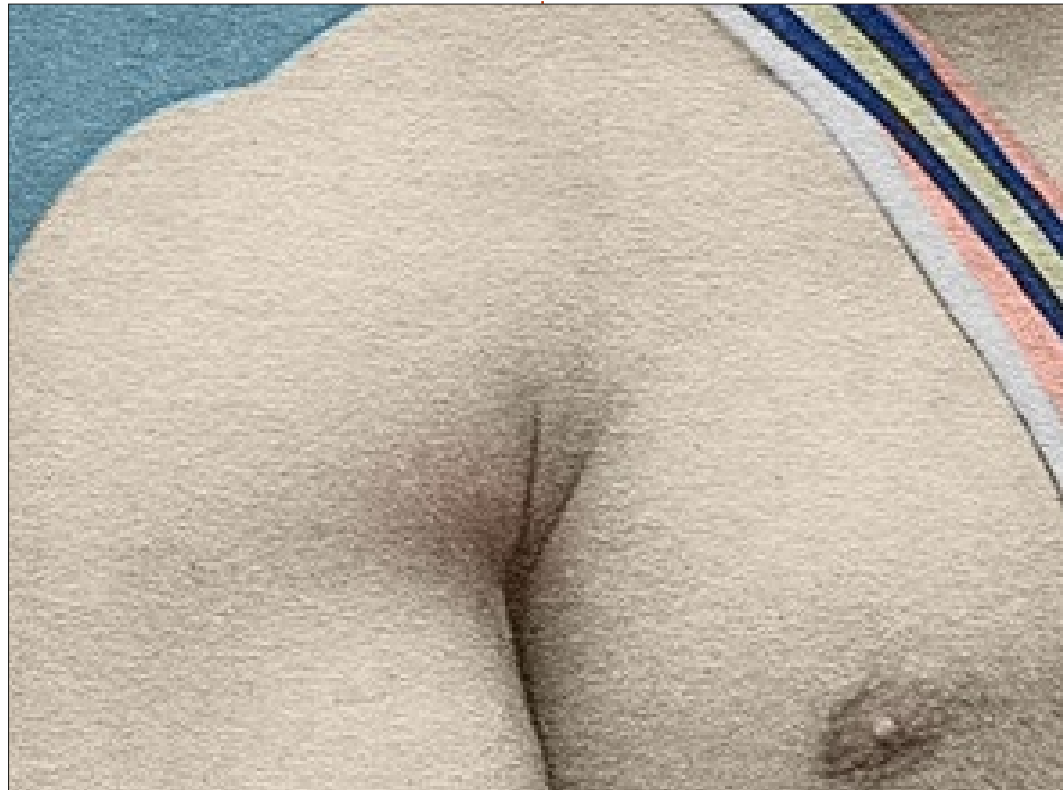


HOWTO - KRITA

possible, I opted for reddish-to-light-brown hair, brown eyes, and a mix of basic colors for the ribbons. With some application, we can get to a result similar to this one. I have been using both the standard “basic-1” brush, and the “airbrush-soft” airbrushes, with small sizes down to 5 pixels. At times, lowering the brush opacity has been of help to do finer details such as, for instance, the subject’s eyebrows. Do not forget details such as the subject’s nipples, which are not quite the same flesh color as the skin around them.



Once we have these basic colors put in, it is a good time to stand back and take a global view of our image. So far, so well, as it is clearly more realistic than the original sepia-toned black-and-white. However, there are a couple of points that need to be improved. In the first place, the subject is clearly of German origin, so the rather dark complexion is not very realistic. A reddish tint would, perhaps, be more typical of people from Northern Europe, specifically when, as an athlete, the subject



would have spent some time out in the open.

To solve this setback, I put in two more layers. One went between the original image and the color layer, and was set to “lighten”. On it, I lightly airbrushed some white (using 20% opacity) on the darker parts of the subject’s face and hands, thus removing part of the shadows that the original photographer had left due to his lighting solution. The second new layer was set up on top of the color layer, as a separate “normal” layer.

On it, I airbrushed --also, lightly-- some red on the same spots. Thus, we get a slightly reddish tinge to facial shadows, and on the arms and hands. Some observations of modern, color, photographs show that this is more “normal” when the subject is a person with a light-colored skin tone.

The other problem can be related to the texture of the photographic paper originally used to print the image. When the postcard was photographed digitally in modern times, the relief on the surface of the paper shows up as a fine corrugation mark, present on the whole surface. It is not especially problematic on the blue background since the backdrop used would have been made of some cloth, and could very well have had some texture to it. But the end result is not very realistic on bare skin, or the metal of the medals.

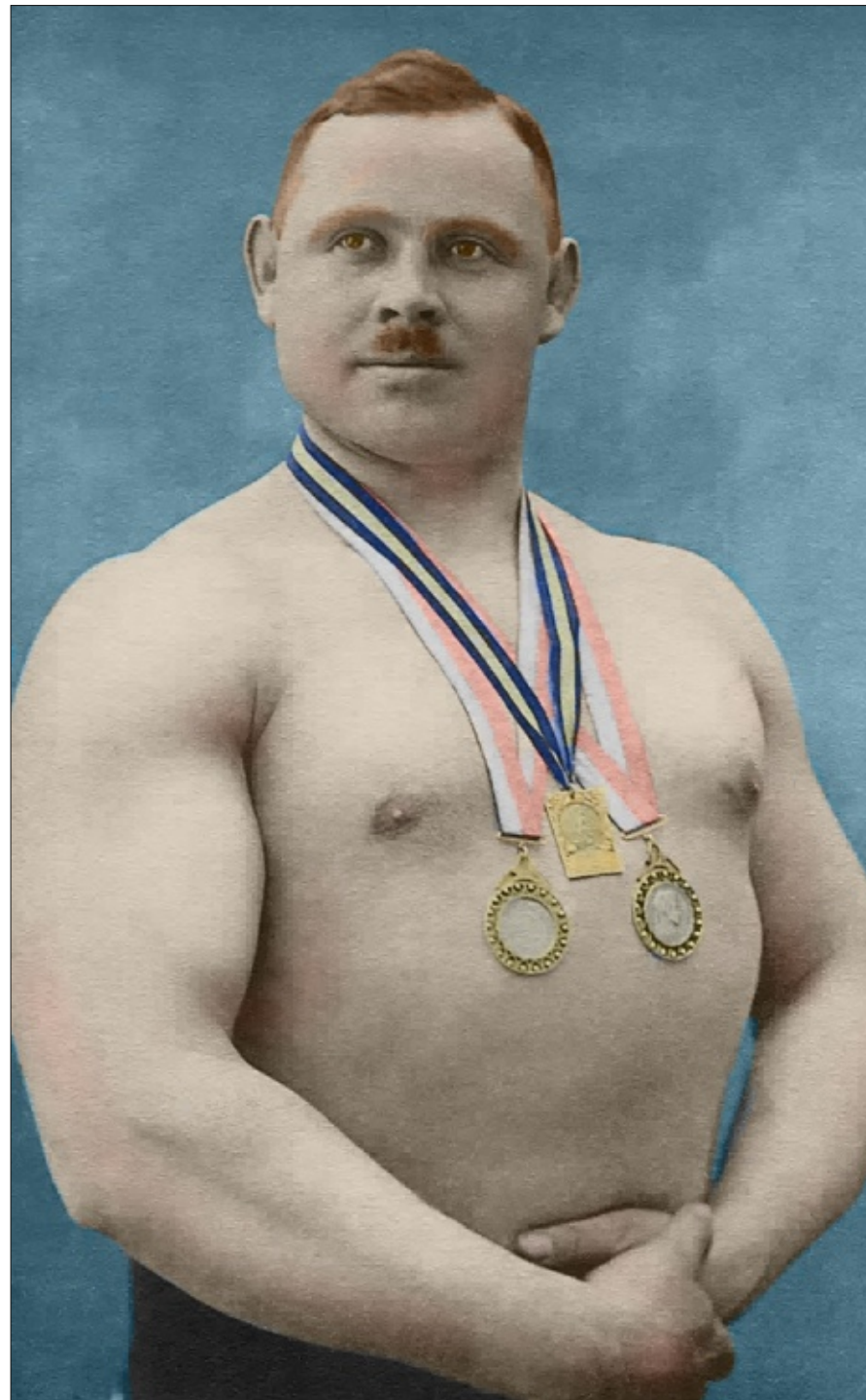
To remove this texture, I worked only on the original image, leaving the color layers as they were. In Krita, there is a tool to do this: choose menu option “Filter”, “Enhance”, then “Wavelet noise reducer”. This has been specifically made to reduce periodic noise

effects in the image. I got good results with a threshold setting of 20, up from the default setting value of 7. The tool cannot get rid completely of the texture without erasing some of the image details, but if used with care can eliminate most of the paper texture.

The final image can then be cropped to suit, and compared to the original: Big Paul now almost seems real once more.

Interested readers may wish to download this photo, and try their own combinations of colors. Which are the most realistic, taking into account the geographical context and time period?

In the next part of this series, we will be working on another portrait -- but this one will not be a photographer's work from the early 20th century but, rather, a very typical effort from the late 1970s when technology had changed and color photography had become more commonplace. Until then, take care!



Alan holds a PhD. He teaches comp sci and eng at Escola Andorrana de Batxillerat. He has given GNU/Linux courses at the Uni of Andorra and taught GNU/Linux systems admin at the OU of Catalunya.

The Daily Waddle

THE DAILY WADDLE

by: ErikTheUnready



Son, what moves you?

W,S,A,D!





Some very interesting events are circulating within the BSD world. Hyperbole is turning to a hardened fork of the openBSD kernel for development. Project Trident left FreeBSD to use Void Linux as their base. Apparently the Linux kernel is being too “wontoon” for security, whereas FreeBSD is difficult for device management.

These two events point towards the intrinsic problem with Linux and BSD kernels and the associated attitude within each community. So there are a lot of items to consider in the future for both operating systems. Do you choose one that is difficult to install? Or do you choose the one that is easy to install, but insecure?

While pondering on this question, I came across nomadBSD. It is based on FreeBSD. It is a persistent live system for thumb drives. It is pretty light on the hardware requirements. And might be a possible alternative to consider for the varying BSD OS on the scene.

I attempted to install nomadBSD previously, but my thumb drive failed to launch on my laptop. The installation instructions seem pretty straightforward, but I’m positive I did something incorrect during setup. I am excited to see nomadBSD on the scene. It can be a viable option for any laptop since it can detect hardware. I only see

about four more columns touching the world of BSD. One will be focused on nomad and MidnightBSD, Project Trident and HyperbolaBSD, and the other minor BSD variants.

About

NomadBSD is a persistent live system for USB flash drives, based on FreeBSD®. Together with automatic hardware detection and setup, it is configured to be used as a desktop system that works out of the box, but can also be used for data recovery, for educational purposes, or to test FreeBSD®'s hardware compatibility.

For a list of installed software packages see the [MANIFEST file](#).

Requirements

The images for 64-bit and 32-bit computers fit on a >=5GB USB flash drive. A system with a 1.2GHz CPU and 1G of RAM should be able to run NomadBSD decently. Booting is possible via BIOS and UEFI.



SJ Webb is a researcher coordinator. When he is not working, he enjoys time with his wife and kids. He thanks Mike Ferarri for his mentorship.



Last month, we got started with the Thunderbird Address Book to help us with basic contact management. This month, we'll look at managing our calendar using the Lightning extension for Thunderbird. This is all in service of the common New Year's resolution to become more organized in the upcoming year. Thunderbird's PIM, or Personal Information Manager, capability can be a big help with that goal.

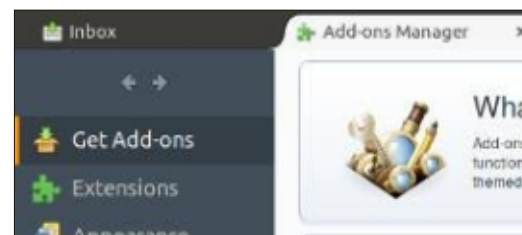
BASIC CALENDAR MANAGEMENT: LIGHTNING EXTENSION FOR THUNDERBIRD

A challenge many of us face – as we age and have health issues (or sometimes as just a function of our personal circumstances, rather than age) – is the need to manage our personal calendars for such things as keeping up with doctor's appointments. Of course, the same principles also apply for work, for anniversaries and birthdays, for personal plans, and for a myriad of

other things we might want to keep track of in our personal calendars. Unlike Microsoft's Outlook on Windows, Thunderbird does not have calendaring built in. Fortunately, the Lightning extension was developed to address this, and is an important addition to Thunderbird's Personal Information Management capabilities.

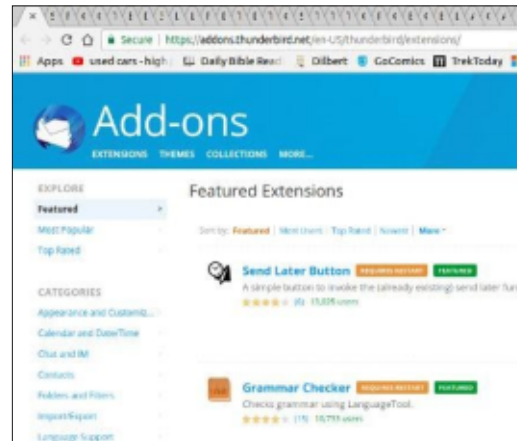
INSTALLING LIGHTNING

To install the Lightning extension to Thunderbird, we'll need to launch Thunderbird first. Go to the Dash (first icon on the Launcher, the strip that runs down the left side of the screen), and type in Thunder. That should be more than enough for the Dash's search capability to bring up Thunderbird. Click to launch it, and you'll get your Thunderbird email client.

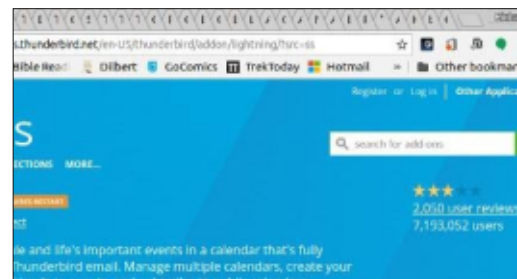


Go to the Tools menu up top, then click Add-Ons.

If you are on a current version of Thunderbird, click Browse all add-ons. A web browser window will open:

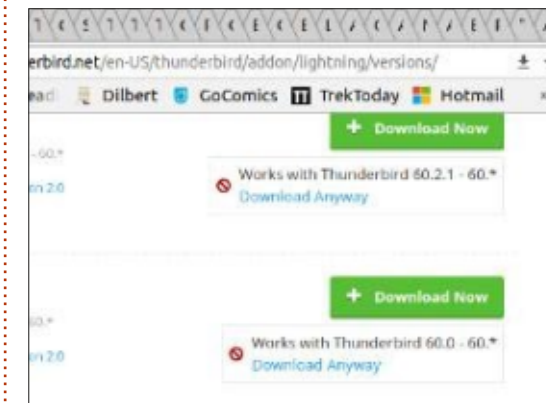


Search for Lightning in the search box at upper-right:

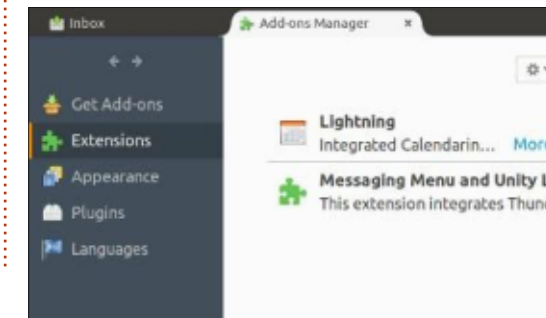


You can click Download Now to start the installation. Now, I have

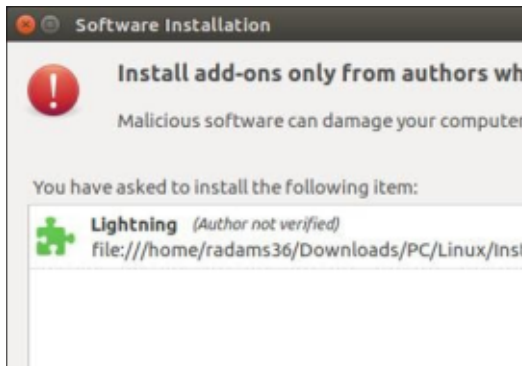
an older version of Thunderbird and did not find it convenient to upgrade right now, so I had to take an extra step. I went to View older versions on the Thunderbird Add-on web page, and found the version that matched Thunderbird 52.2.1. I then downloaded the XPI format file and saved it to my Download folder.



Then, I had to go to Thunderbird's Add-Ons under Tools again and select Extensions:



Click the Gear icon at the top and select 'Install add-on from file'. Navigate to where the XPI file was saved and double-click it. The Add-On Manager will now install the add-on. This is good to know for other installations, as XPI format files are commonly used for Add-Ons found outside the official Thunderbird support pages. You will want to click Install Now on the dialogue box that comes up:

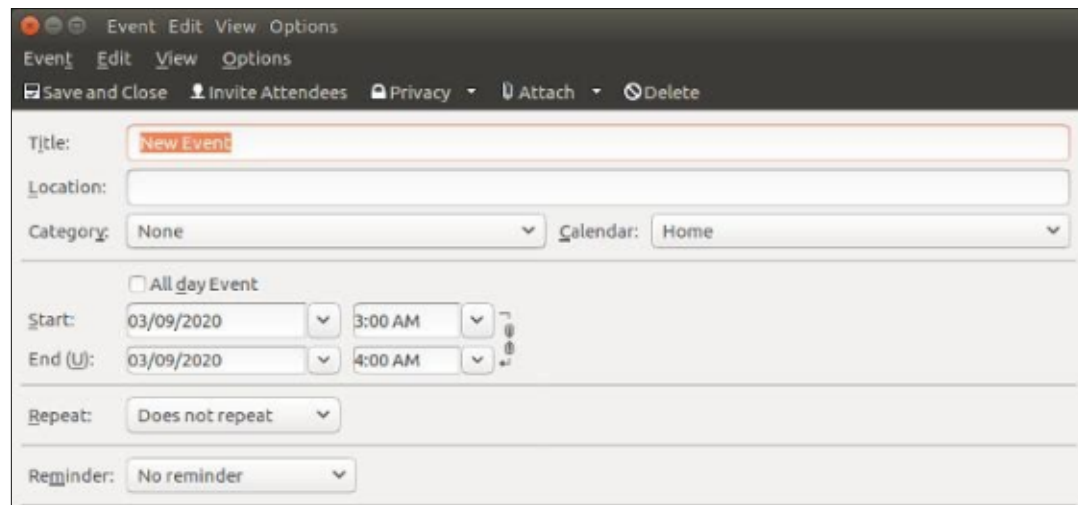
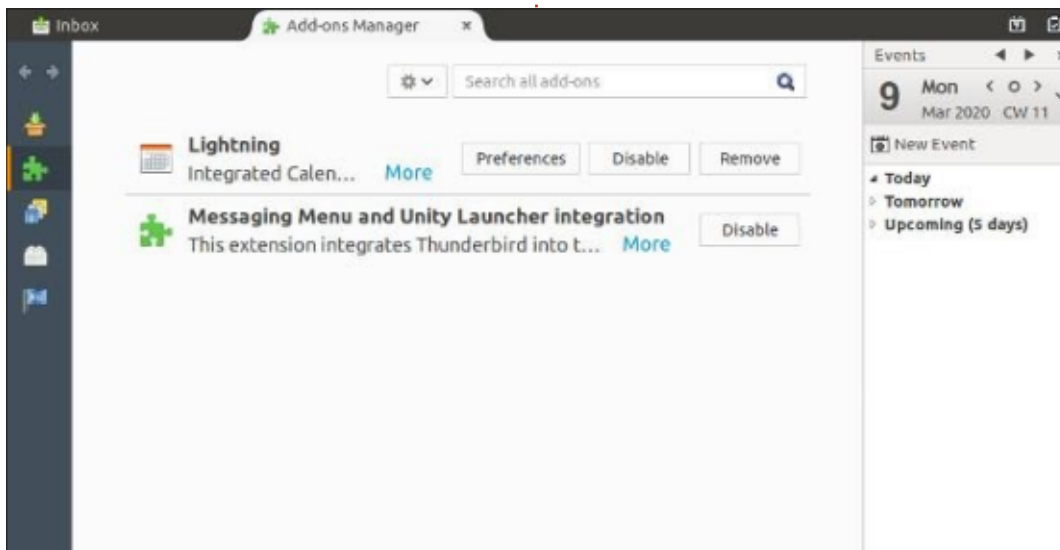


YOUR NEW THUNDERBIRD INTERFACE

After the installation of the add-on, Thunderbird will prompt you to restart the application. Once you've done so, you'll see a new pane to the right showing your current day's events and appointments:

Press Keep at the bottom to let Thunderbird know you want to continue using the Lightning add-on. Click the X on the Add-On Manager tab to shut it down and return to the main Thunderbird interface, which will still have the new Lightning pane:

Add new events to your

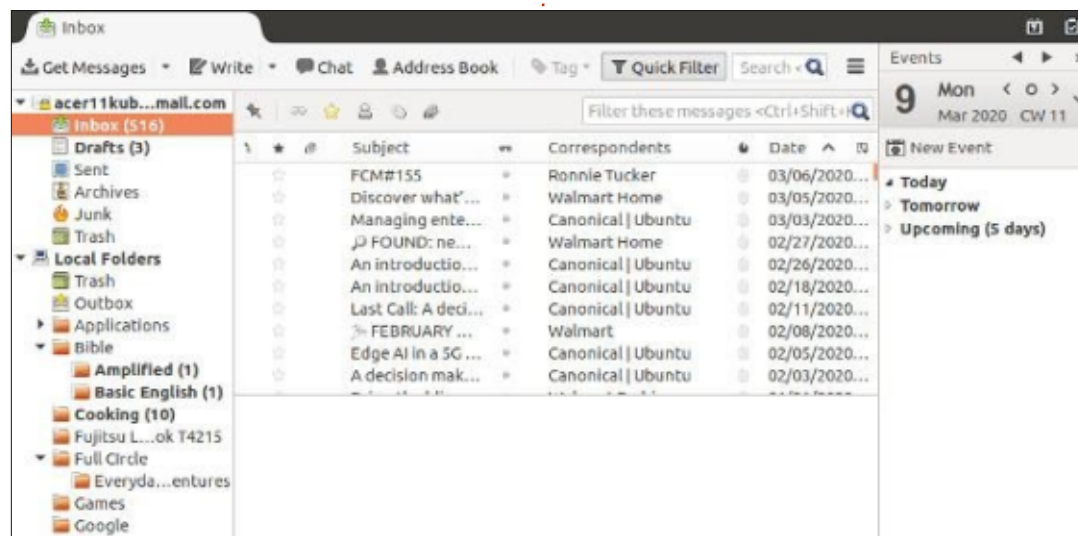


personal calendar by clicking New Event in the upper right and fill in the information for your event as appropriate:

Next month: Connecting Lightning to Google Calendar.



Richard 'Flash' Adams spent about 20 years in corporate IT. He lives in rural northwest Georgia, USA, with his adopted 'son', a cockatiel named Baby.

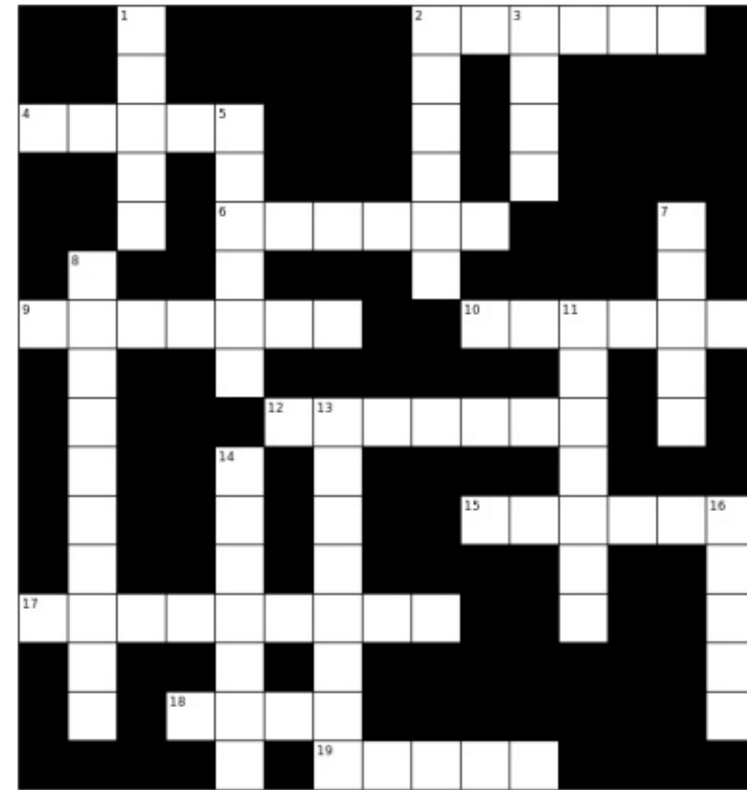




UBPORTS DEVICES

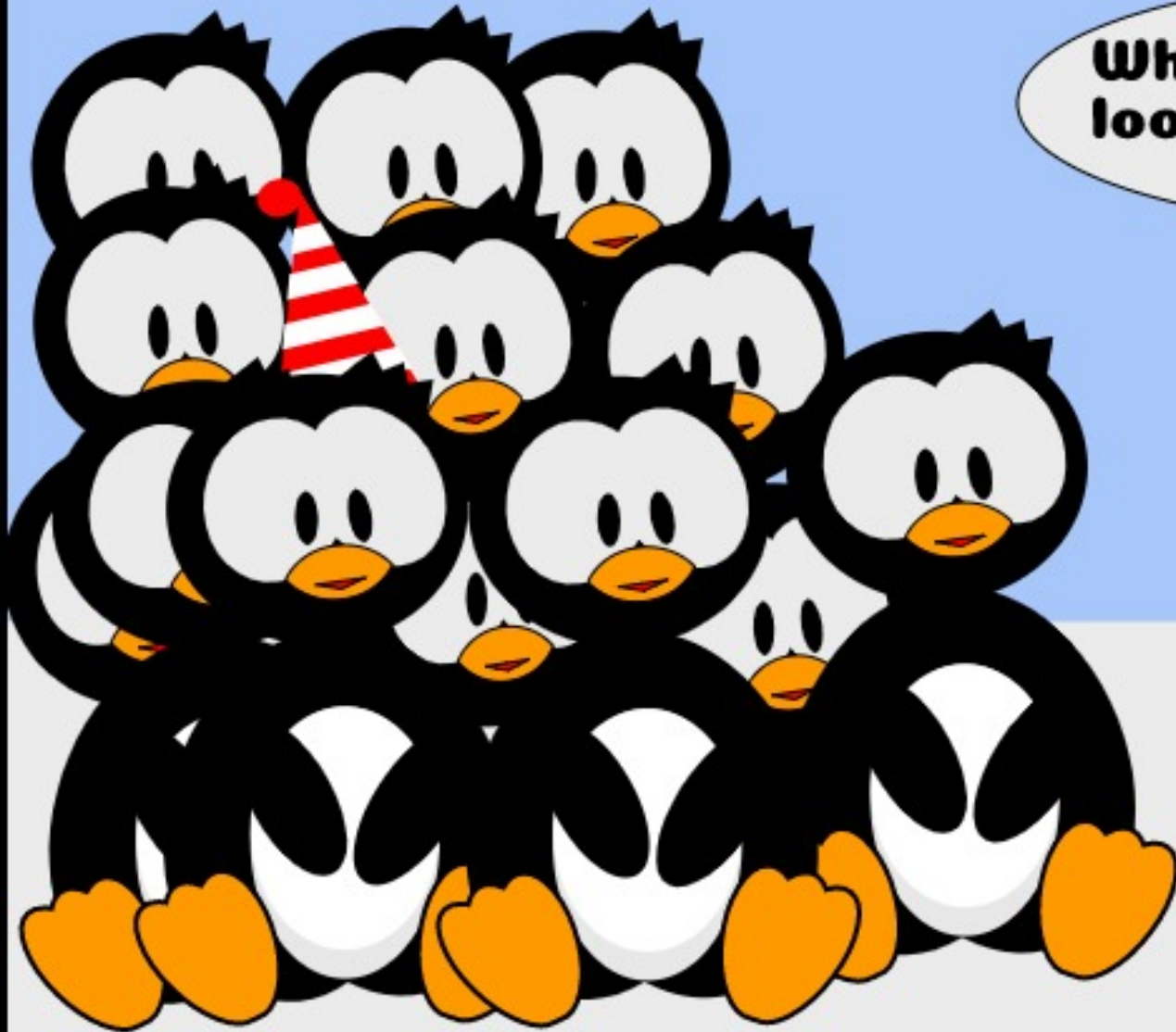
Written by UBports Team

COMING SOON



- 1D. Provided by Stamus networks, ready to use Suricata IDS/IPS ecosystem.
- 2A. Try it, this could be fun too?
- 3D. Sponsored by the state of Cuba, based on Ubuntu. (Previously based on Gentoo).
- 4A. "Linux for the lazy Slacker" when you see the bonsai tree you will know.
- 5D. Debian... with XFCE, made to look like warty warthog.
- 6A. Like a Japanese meal, based on 2A.
- 7D. Discontinued BSD distro for SPARC and x86.
- 8D. You can suck it...
- 9A. What monks do...
- 10A. Like the Pagani mid engine sports car...
- 11D. Eyecandy German OS that may come from Alpha Centauri.
- 12A. A Linux school project client.
- 13D. Jennifer Saunders would say it's "fabulous".
- 14D. Resurrection of Cub Linux.
- 15A. Home entertainment system built on Linux.
- 16D. Not the programming language or Taylor.
- 17A. Just enough OS for Kodi.
- 18A. Goes well with Lamb.
- 19A. Where Enlightenment marries Debian.

The Daily Waldo Waddle



Why do I feel like I am looking for someone?





This article covers my experience (so far) of Ubuntu 18.04 – including when I purchased a new Dell laptop at the end of 2019. Specification = Inspiron 15.6 inch model 3581, with 8GB RAM, Intel 7th Gen Core i3 Processor + Tray load DVD device. As you will see, my first introduction to Ubuntu 18.04 was quite drastic.

A BIT OF BACKGROUND.

For what seems like forever, I used an HP laptop running Windows Vista, not updating to 7, 8, or even Windows 10. When the hardware was getting very slow, my thoughts were ‘If I have to learn Windows 10, why not learn LINUX?’. After some investigation, I determined that Ubuntu looked to be the best for a home user to learn.

I purchased a Dell laptop in 2016 running Ubuntu 14.04, and started to understand that Ubuntu could be very useful. Due to my lack of Linux experience, I set up a Standard user account, without any password, to use on a day-to-

day basis, without administration rights, so that I could not inadvertently issue disastrous commands.

In 2017, the laptop generated a fault that was fixed by Dell; on its return it had the new Ubuntu 16.04 installed. When Ubuntu 18.04 was released, I read up about it and thought that I could investigate it by booting the 18.04 version from a USB stick, as there was no DVD/CD device on my laptop.

After reviewing a number of web explanations of how to run from a USB stick, I attempted to make a bootable Ubuntu 18.04 USB stick. In the end, I had to use both the Ubuntu 16.04 and Windows Vista laptops to get a bootable USB stick. Finally, the Ubuntu 18.04 opened up on my Dell laptop screen. After my review, I then found that I could not get back to using my laptop in version 16.04, but, unfortunately, I could not update to 18.04 either. Something had gone wrong with the GRUB2 file, whatever that was, and whatever I tried I could not

overcome the problem.

The boot up process was trying to use the Extensible Firmware Interface (EFI) and, due to my lack of understanding, I tried to find information from the web as well as purchasing ‘The Official Ubuntu Book’, but had to revert back to booting up using Basic Input/Output System (BIOS) and Master Boot Record (MBR).

So I waited until I could afford to purchase a new computer with Ubuntu 18.04 already installed.

BACK TO THE NEW LAPTOP AND UBUNTU 18.04.

When the new Dell computer was delivered, the Ubuntu 18.04 software install process asked if a recovery disk was required – which I confirmed, thus the operating system setup started. Other requests asked for user account(s) to be set up – and I found that all accounts now have to have passwords, and the Guest account was no longer installed as part of

the operating system.

After Ubuntu 18.04 was up and running, I wanted to check if there were any updates available / required and found that by opening ‘System Settings’, then looking under the heading ‘Details’, there was the option ‘Check for updates’. Over a few days, and on a number of occasions, I clicked on this option and was told my system was up-to-date – which I found strange!

Due to my previous experience with Ubuntu 18.04, I was interested in finding out how the hard disk had been configured. While trying to get my old 16.04 laptop to boot, I found GParted Partition Editor very useful, so tried to run it under 18.04.

Unfortunately I could not find it, so I looked on the web to be told that there were two ways to install GParted, either using ‘Ubuntu Software’ or using ‘sudo’ at the command prompt in a terminal window.

The 'Ubuntu Software' could not find GParted and the only way I could install it was to use 'sudo' commands at a Terminal prompt. The commands installed, checked, and started the GParted Partition Editor.

What also happened was that a window opened automatically stating that there were 18.04 Software Updates required. Why had the 'Check for updates' informed me that the system was up to date?

During the download of over 800MB of data, another window opened with the title of 'What Do You Want To Do About Modified Configuration File GRUB = /tmp/grub.BcD6fzbae1 of configuration file /etc/default/grub is available, but the version installed currently has been locally modified'. (Aha, that file called GRUB again. Pls note I had not modified this or any other files). There were a number of options offered, the one that I clicked on was [Show a side-by-side difference between the versions]. The screen closed and I was expecting the two files to be displayed, but the software updates continued without any

other warnings / options, etc. As expected, at the end of the updates, the system needed to be restarted.

After looking around the desktop of Ubuntu 18.04, I could not find anywhere to display the battery status on the menu bar as a percentage. So back on to the web.

I found that one needs to install GNOME Tweaks to be able to display the battery status on the top menu bar. The screens that are displayed when Ubuntu 18.04 is up and running are known as the desktop – which is controlled by the GNOME manager. Apparently there are a number of different desktops available for the Linux operating system.

To install GNOME Tweaks, we are back to using 'sudo' commands at a Terminal prompt.

In the fullness of time, I hope to understand why, after using the 'sudo' commands at a Terminal prompt to 'install' the GNOME Tweaks, one has to install the application a second time when trying to open the application with either the 'Show Applications' or

'Supper' key (a.k.a. Windows key).

I now appreciate that the operating system has to be rebooted to see new installed items listed under the Installed heading in Ubuntu Software. I also note that each user has to update their desktop environment.

My next tasks will be to install a few more of the applications that I have used in the past.



Wil Lake is a retired time served mechanical engineer who retrained as an IT engineer when Microprocessors entered the mainstream. He has worked in the IT industry for over 30 years, lives in the Cotswolds England UK, and has spent years renovating a cowshed.



GUIDELINES

The single rule for an article is that **it must somehow be linked to Ubuntu or one of the many derivatives of Ubuntu (Kubuntu, Xubuntu, Lubuntu, etc).**

RULES

• There is no word limit for articles, but be advised that long articles may be split across several issues.

• For advice, please refer to the **Official Full Circle Style Guide:** <http://bit.ly/fcmwriting>

• Write your article in whichever software you choose, I would recommend LibreOffice, but most importantly - **PLEASE SPELL AND GRAMMAR CHECK IT!**

• In your article, please indicate where you would like a particular image to be placed by indicating the image name in a new paragraph or by embedding the image in the ODT (Open Office) document.

• Images should be JPG, no wider than 800 pixels, and use low compression.

• Do not use tables or any type of **bold** or *italic* formatting.

If you are writing a review, please follow these guidelines :

When you are ready to submit your article please email it to: articles@fullcirclemagazine.org

TRANSLATIONS

If you would like to translate Full Circle into your native language please send an email to ronnie@fullcirclemagazine.org and we will either put you in touch with an existing team, or give you access to the raw text to translate from. With a completed PDF, you will be able to upload your file to the main Full Circle site.

REVIEWS

GAMES/APPLICATIONS

When reviewing games/applications please state clearly:

- title of the game
- who makes the game
- is it free, or a paid download?
- where to get it from (give download/homepage URL)
- is it Linux native, or did you use Wine?
- your marks out of five
- a summary with positive and negative points

HARDWARE

When reviewing hardware please state clearly:

- make and model of the hardware
- what category would you put this hardware into?
- any glitches that you may have had while using the hardware?
- easy to get the hardware working in Linux?
- did you have to use Windows drivers?
- marks out of five
- a summary with positive and negative points

You don't need to be an expert to write an article - write about the games, applications and hardware that you use every day.





Review: QNAP NAS

Website: <https://www.qnap.com>

Price: \$500-2000 (depending on the model)

From the web page: *QNAP Systems, Inc., headquartered in Taipei, Taiwan, provides a comprehensive range of cutting-edge Network-attached Storage (NAS) and video surveillance solutions based on the principles of usability, high security, and flexible scalability. QNAP offers quality NAS products for home and business users, providing solutions for storage, backup/snapshot, virtualization, teamwork, multimedia, and more.*

I have been adding a lot of QNAP NAS products for clients in the past two years, and I thought I would share my experiences with you. If you already have a NAS set up, or your own server, you can probably skip this article. The QNAP NAS, however, is fully loaded with features, so if you

have ever battled setting up your Ubuntu server with SAMBA and DLNA, etc, this may be for you.

THE UNITS:

I have mostly been installing two- and four-bay NAS units as most of my clients use it for backup rather than all of the other built-in features. That said, there are bigger units available, six- and eight-bay NAS units are not uncommon. The feature set is quite extensive. The units have a

metal chassis covered by a plastic shell. They are not meant to stack, but will sit on top of each other without an issue. The units also ship with two network ports, so connection is a breeze. The power supply is not built in, rather it is a laptop power supply, so the units are not heavy. The shell comes in more than just black, so you can put it on a shelf in the office and it will blend right in.

As with most NAS boxes, you have to buy your own drives, so do

your sums before purchase. The units do not have an abundance of RAM or CPU power, but it handles encryption and other tasks seamlessly.

SET UP:

You have two options here, once you have screwed your drives to their caddies and clicked them home. You can use the software provided, or you can configure it via a web page, if it is on your network. You can have your drives

TR Series

Hardware RAID Storage Expansion Device for both PC and NAS



separate, or in a RAID configuration. Because it is Linux under the hood, you can have logical volumes set up. Setting up accounts and permissions is very simple and straightforward, and there is an overview (dashboard?) to see who can do what. Adding applications is like using the Ubuntu store, you pick one and install it. QNAP have also made management from the internet easy with a handy QR code on the outer shell. Everything is very intuitive, but help is never more than a click away should you get stuck. Setting up the NAS is really a pleasure, and I would encourage you to poke around, as everything has tool tips and hints and you cannot really break it at setup time.

USAGE:

As previously stated, my client's main use is backup. Since Qbackup is provided free of charge, this alone can justify the purchase of one of these units. Qbackup is a basic solution, but gives you everything you could need including email notifications for home users and small business users. The unit also has USB ports

if you want to connect another USB drive to it, to back up your data, should you wish to. The unit is also an excellent music server and photo repository, integrating with your computers and mobile devices on the local network and even across the internet. The interface is reminiscent of an Android tablet, so anyone should be able to use it. Once you have it set up the way you like it, the only time you will ever interface with it directly would be to update firmware or add new features. Once it is working, it will get out of your way and operate flawlessly. The tiny fan is really quiet and there are only two small LED's, so you do not have a disco going at night. (Unlike other brands like Synology where you need sunglasses at night to counter all the blinking lights).

THE APPLICATIONS:

These guys have literally thought of everything. There are applications in the store for music streaming, video streaming cloud storage, torrent seed boxes, Plex servers, etc etc. You actually have to have a look at all the options to comprehend it. All these

applications are add-ons to your NAS that extend its usefulness and value, not only to the home user but also to the business user. I have still to see if the enterprise class devices have the same add-ons available, but I have not used any of those.

THE 'APPS':

As my iPad is out of date (I do not plan on updating it as Apple just introduces slowing down routines to force you to buy new), I can not comment on AppStore applications, but I will endeavour to talk about the Android ones here.

Mostly I use Qmanager and Qfile. The first to manage the device and the second to check on backed up files. Now you can also use your NAS for other things, like streaming music and video, backing up your mobile devices, or CCTV footage storage. Just like the joke, I can say: "there is an app for that!".

Do yourself a favour and open the Google Play store on your Android device and search for QNAP. There are, at the time of

writing, more than 20 QNAP 'apps' for Android. Almost every use case is covered and the 'apps' are updated regularly.

Pros:

- QNAP provides lots of Android 'apps' for you to interact with your NAS when you need to.
- The units are under active development and new firmware is pushed out like clockwork. You can do a firmware upgrade via your mobile via the internet.
- The applications are constantly being improved and they too see regular updates.

Cons:

- If you have power issues, there is no way to do a disk check remotely.
- If you have not logged in for a while, you will get locked out until you confirm via email.
- The unit has a horrible shrill tone when there is an error (or it reboots), so keeping it in your bedroom or office can cause quite the heart attack when it is quiet.



LETTERS

If you would like to submit a letter for publication, compliment or complaint, please email it to: letters@fullcirclemagazine.org. PLEASE NOTE: some letters may be edited for space.



Join us on:

goo.gl/FRTML



facebook.com/fullcirclemagazine



twitter.com/#!/fullcirclemag



linkedin.com/company/full-circle-magazine



[ubuntuforums.org/forumdisplay.php?f=270](https://ubuntuforums.org/forum/display.php?f=270)

FULL CIRCLE NEEDS YOU!



Without reader input **Full Circle** would be an empty PDF file (which I don't think many people would find particularly interesting). We are always looking for articles, reviews, anything! Even small things like letters and desktop screens help fill the magazine.

See the article **Writing for Full Circle** in this issue to read our basic guidelines.

Have a look at the last page of any issue to get the details of where to send your contributions.



DistroWatch.com

Put the fun back into computing. *Use Linux, BSD.*



Q&A

Compiled by EriktheUnready

If you have a Linux question, email it to: questions@fullcirclemagazine.org, and Erik will answer them in a future issue. Please include as much information as you can about your query.

Welcome back to another edition of Questions and Answers! In this section, we will endeavour to answer your Ubuntu questions. Be sure to add details of the version of your operating system and your hardware. I will try to remove any personally identifiable strings from questions, but it is best not to include things like serial numbers, UUID's or IP addresses. If your question does not appear immediately, it is just because there is such a lot, and I do them 'first-come-first-served'.

Back in the day, we didn't have Sean Connery... oh wait, we did. What we didn't have was high speed internet, so, when this new-fangled technology rolled around, there were some people who saw an opportunity to use it for good. They installed a 9600baud modem in a PC to be able to do accounting and stock-take in one location. The PC was wrapped in metal, with a keypad and tiny green display. It was sold as a till and accounting system. However, the units were installed in places where the humans were an issue, so the

engineers came up with a plan to change the pin layouts of the phone jacks, and the cables for the modems. Because lightning on the telephone lines damaged the modems, they needed someone to go replace them, if faulty. Enter yours truly. Arriving at these stores, usually in high streets, carrying tools and replacement parts, after pushing through throngs of people, I would often find no fault. Turns out, the employees wanted to use the phone jacks to make free phone calls. Failing to do so, the pins not being standard, they would leave it unplugged, hoping a technician would arrive and tell them how to make free phone calls. What I am trying to illustrate here is: there is always the human factor. Have you checked the human factor before posting on a forum or chat?

Q: I have Xubuntu. I have been thinking of going to Disco Dingo for fractional scaling, e.g 1.25x. Deepin looks like it supports it, and maybe KDE too. Can I backport it to 18.04? I have a 50

inch TV that I have connected, but some things are just too small to see. I wear spectacles already. My media PC is actually an old laptop connected to my TV via VGA port, not HDMI.

A: I understand the part of not wanting to reload in 9 months. If you use a laptop, do you have an external mouse and keyboard attached to control it with? If so, why not use the mouse wheel and left ALT to zoom in when having to read or type, and zoom out again to watch your movie? It will zoom to your pointer. You can make your pointer bigger in settings > mouse > themes > cursor size.

Q: How do I do wa -la? I have man, but no entry. I posted the question to stack exchange and the answer was to sudo Nautilus and navigate wa -la. Did he mean ls -la? I would like to retrieve file from a standard account I can't log into. I need to type some commands in terminal

or go through the files app to access the file.

A: I have never heard of wa? It could be ls -la. I would suggest the find command.

EDIT: I think I found your post ! What the guy was trying to say was VOILA! (wa-la) :D

Q: I've installed Ubuntu 19.04 on my Thinkpad. But I can't use my touchpad? Ubuntu can see it, so it should work. I am using an external mouse atm, so it is not a big deal. Can you help me? This is my output:

```
$ xinput list
Virtual core pointer
id=2 [master pointer (3)]
Virtual core XTEST pointer
id=4 [slave pointer (2)]
Microsoft Microsoft® Nano
Transceiver v2.0 id=10 [slave
pointer (2)]
Microsoft Microsoft® Nano
Transceiver v2.0 id=11 [slave
pointer (2)]
ETPS/2 Elantech Touchpad
id=15 [slave pointer (2)]
```



A : Two questions: is it enabled in your settings panel? Do you perhaps dual-boot and maybe use software on the windows side to turn it off? (I am assuming you have tried the shortcut keys on your keyboard to try and turn it on again).

Q : Which Office package is best? I have heard a lot of hype surrounding WPS Office.

A : Best is subjective, but I am glad for this question. You see last week I lost the WHOLE Q&A section due to an issue with OnlyOffice, so I am back to LibreOffice again. For bog standard letters, any of them will do. I will address WPS Office first as it was your question. WPS Office has a free and paid option. The free option is slightly crippled (like OnlyOffice too). WPS office is not open-source. Though the program is a pleasure to use, it phones home all the time, which is the part I do not like. If you install it offline and use it offline, it is quite fine. For features such as versioning,

you cannot beat the price of LibreOffice (though it may look outdated.)

Q : I have bought a new laptop with Windows10 preinstalled. I have tried it and hated it. There is no control, and it installs crap I don't want and never asked for, and what even are these sh#tty "suggestions" ? My problem is that this laptop is tiny and has one USB port, no DVD drive. How do I install Ubuntu? No dual-booting please. Wipe this crap off the face of the earth.

A : If your laptop has a card reader slot, you can create a bootable disk on an SD card and install from there. I am assuming the USB port is in use. On windows, you can use Rufus to make it, and on Linux, Balena Etcher. I am not going to hold your hand through the install, but point you here: <https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-desktop#0>

Q : I have a dual-boot (windows 10 and Ubuntu 18.04) machine. I have 3 partitions, one for windows, one for Ubuntu, and one for both. I just formatted that partition as NTFS from windows, I could only see it from Ubuntu. I could not write to it. Then I formatted it using Ubuntu. After that I could read and write using Ubuntu. Then, I saved a file on it using windows. Then I was back to square one. What can I do? With best regards.

A : Actually, you have many options. Shutting down windows by holding down the SHIFT key when pressing the shutdown icon. This shuts windows down and does not leave filesystems in use. (Hibernating). Turning off hibernation completely. Etc. But all the fixes are all on the Windows side.

Q : I have a failing SD card. I want to save as much as possible. I heard that Gparted has 'attempted rescue', and dd will make an image of the card. Which is best?

A : This time I can say neither. Can I suggest you look at photorec (not just for photos) before you clone the SD card? Recover as much with this utility before you do the other ways you have heard about, and maybe use ddrescue instead of plain dd.

Q : Is there a way for me to extract audio from a youtube video?

A : Yes! One way is to use an online converter, there are many of those, or youtube-dl, or even VLC!

Q : Hello. I switched from Ubuntu to MX to see what the fuss was about. It seems to be a storm in a teacup. I can't seem to install any of my favourite software, it's just not found? I can't uninstall stuff properly as there is no software centre to uninstall stuff like flash that I don't want. It feels like a relic from a bygone era.

A : Your question? (Switch back to Ubuntu, or try Voyager).

Q: What is this sorcery? I installed the latest iso and now my laptop won't charge in ubuntu. It remains or runs down, never up. I tested in windows and it does charge. I don't even know where to start looking.

A: Usually the fault is at Microsoft's door. In Windows, discharge the battery completely and charge it full again, or do a battery calibration with the vendor software. Now boot to Ubuntu and try again. Also see if it charges when you turn the machine off. Update your machine BIOS and the Linux kernel. Uninstall TLP, if installed, and try without it.

Q: Hello friends. How can I see what is eating my bandwidth? Here in India it is a problem. I need to tell who is the problem.

A: Hi, run:

```
sudo apt install nethogs
```

and, once installed, run: `sudo nethogs` - IF you have more than one interface, you need to specify which one.

Q: So, after updating from Ubuntu 18.10 to 19.04, Xfce terminal can not be started from the Panel. "Failed to launch preferred application for category TerminalEmulator. Failed to execute child process /usr/lib/x86_64-linux-gnu/xfce4/exo-1/exo-helper-1 (No such file or directory) Directory exo-1 does not exist." This error is popping up everywhere. What went wrong?

A: I cannot say what went wrong, but I can tell you that the error tells you what is wrong. Open a terminal and type: `sudo apt install libexo-1-0`

Q: How can I get night light from Ubuntu Gnome to Xubuntu? The bright screen really messes with my eyes and my roommate is complaining about his sleep patterns.

A: There are two options: 1. Redshift, 2. F.lux.

Q: Desktop sounds being back is great for home, but not for work. Where can I kill it?

A: Install dconf editor then `gnome > desktop > sound` and make it false.

Q: I moved from Gnome to XFCE. I am a bit shaky on my feet. I see the battery indicator shows my wireless mouse battery, but it remains on 75% even when new or flat. I don't recall this in Gnome.

A: I do not have a definitive answer for you other than the mouse's Linux support is lacking. You can try to get a driver from the manufacturer. Consider yourself lucky, mine does not even see my mouse's battery.

Q: I have a new PC Windows 10 64-bit, AMD Ryzen 3 2200G, with Radeon Vega 8 Graphics, 8.0 GB RAM, Motherboard MSI B350M PRO-VDH. When I installed Linux Ubuntu 18.04, all was OK, as usually in the past. When I restarted, the PC had a crash. When I installed Windows 10 Home after restart all was OK. Could you explain me why Linux is for this HW forbidden? How can I find out it in advance? In documentation of producers, I did not find it. Thanks for solving.

A: Right, nothing is forbidden, though MSI is known to be a Windows-only house. I think you can try Ubuntu 18.10 or 19.04 rather, as the problem is Ryzen CPU support. The Ubuntu 18.04 image you are booting from may be too old? Have you tried Ubuntu 18.04.2? Also, see if there is updated firmware or BIOS for that motherboard. If you would like to know in advance which hardware is Ubuntu certified, you can check out this web page: <https://certification.ubuntu.com/desktop/>

Q: I have installed Anki on Disco Dingo. I use it for uni. However, it's not working. I need to get going soon.

A: You are going to have to build it from source. The version by Ubuntu is too far behind. (If you do not know how, mail me back and I can walk you through it).

Q: I have installed virtualbox and added the Ubuntu ISO file as a fake CD. It boots quite fine. Why would I need to install it?

A: Running from a live DVD / ISO is also fine. If you want to know why you cannot run it live, you can, by all means! That is one of the software freedoms you have with free software. Unless I am understanding your question wrongly.



Erik has been in IT for 30+ years. He has seen technology come and go. From repairing washing machine sized hard drives with multimeters and oscilloscopes, laying cable, to scaling 3G towers, he's done it.





Website: <http://asciiicker.com/y2/>
Author: Gumix

Current version: y2 [You can see previous incarnations by replacing y2 with y1 or y0. You can see previous versions in the X-range by replacing the y2 with say, X13].

Do you spend a lot of time at the terminal? Are you used to seeing "yourself" as an @-sign? Do you like ASCII games? Well, then you may drool over this. This is the geekiest thing I've seen in a while. The whole thing is rendered in text. When I say "whole thing", I mean a 3D world! Forget Zelda.

When I think of DOS ASCII games, I usually envision ZTZ-type graphics with that horrible smiley face. This takes ASCII to the next level. When I say next level, I mean there is even a multi-player mentioned! The rendered text is fed to a Javascript engine and turned into 3D. This means you play in a browser, but there is footage of it being played in a terminal, kiTTY. (Whoo-hoo!).

To actually test in your browser, simply load the page and press the arrow keys. You can also use W,A,S,D. Q and E rotate the camera. The space-bar jumps. You can even click the character around with the mouse. There is a lot of attention to detail; for instance, when your character enters the water, he will go deeper until he swims. You can collide with objects, and there are basic

shadows. There is no story yet, and y2 is to show off the falling-down animation, so, if it bothers you, choose y0 or y1.

Don't think this is a flash-in-the-pan though; there are development tools for this "game" that, they say, will be open-sourced. Be aware that it is not open-sourced yet. I use "game" in quotes as this is more of a proof-

of-concept at the moment. New things are implemented in every version. X13 brought us some "crazy semi-procedurally generated map". There is even terrain now. If you go down to the pond, you will slide down the "embankment". When you go to the boat, you can fall off the rocks. As you can see in the latest incarnation, the "game" is leaning towards a medieval RPG, with



UBUNTU GAMES - ASCIICKER

swords and armour.

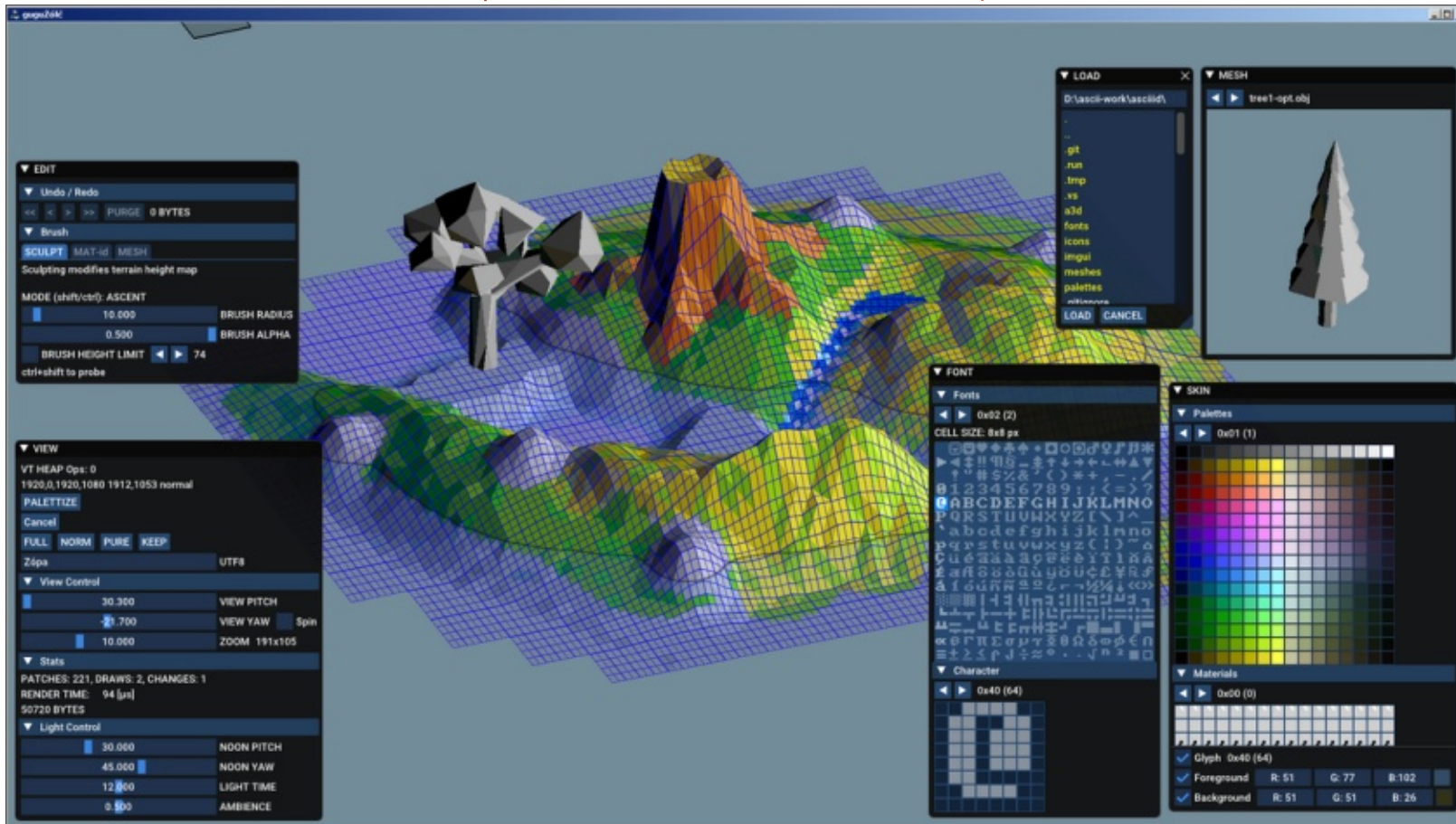
This has really sparked my imagination, and I hope it sparks yours too. I am not sure if it's just the project is so way out, or the idea that something like this is possible in a terminal that has my wheels spinning. Either way, I will be following with glee. I cannot wait for the lot to be open-sourced as I would LOVE to use this to make a modern... ASCII... version of

Cyclone
<https://en.wikipedia.org/wiki/Cyclone>
[ne \(video game\)](https://www.youtube.com/watch?v=...)

Go on, what are you waiting for?
Go try your hand at ASCIIcking!

We wish Gumix / Gumiks all the best with his ambitious project.

You can follow the project on
Reddit -
<https://www.reddit.com/r/asciicker/new/>



Erik has been in IT for 30+ years. He has seen technology come and go. From repairing washing machine sized hard drives with multimeters and oscilloscopes, laying cable, to scaling 3G towers, he's done it.



PATRONS

MONTHLY PATRONS

Alex Crabtree
 Alex Popescu
 Andy Garay
 Bill Berninghausen
 Brian Bogdan
 CBinMV
 Darren
 Dennis Mack
 Devin McPherson
 Doug Bruce
 Elizabeth K. Joseph
 Eric Meddleton
 George Smith
 Henry D Mills
 Hugo Sutherland
 Jack
 Joao Cantinho Lopes
 John Andrews
 John Malon
 John Prigge
 Jonathan Pienaar
 JT
 Kevin O'Brien
 Lee Allen
 Leo Paesen
 Linda P
 Mark Shuttleworth
 Norman Phillips
 Oscar Rivera
 Paul Anderson

Paul Readovin
 Rob Fitzgerald
 Roy Milner
 Scott Mack
 Sony Varghese
 Tom Bell
 Tony
 Vincent Jobard
 Volker Bradley
 William von Hagen
 Taylor Conroy

SINGLE DONATIONS

2020:
 alex moro
 Ronald Eike
 ALEXANDRU POPESCU
 Linda Prinsen
 Glenn Heaton
 Jon Loveless
 Frank Dinger
 Raymond Mccarthy
 Daniel Rojo
 Frits van Leeuwen

The current site was created thanks to **Lucas Westermann** (ex-Command & Conquer) who took on the task of completely rebuilding the site, and scripts, from scratch, in his own time.

The Patreon page is to help pay the domain and hosting fees. The yearly target was quickly reached thanks to those listed on this page. The money also helps with the new mailing list that I set up.

Several people have asked for a PayPal (single donation) option, so I've added a button to the right side of the website

A big thank you to all those who've used Patreon and the PayPal button. It's a HUGE help.



<https://www.patreon.com/fullcirclemagazine>



<https://paypal.me/ronnietucker>



<https://donorbox.org/recurring-monthly-donation>



HOW TO CONTRIBUTE

FULL CIRCLE NEEDS YOU!

A magazine isn't a magazine without articles and Full Circle is no exception. We need your opinions, desktops, stories, how-to's, reviews, and anything else you want to tell your fellow *buntu users. Send your articles to: articles@fullcirclemagazine.org

We are always looking for new articles to include in Full Circle. For help and advice please see the **Official Full Circle Style Guide**: <http://bit.ly/fcmwriting>

Send your **comments** or Linux experiences to: letters@fullcirclemagazine.org
Hardware/software **reviews** should be sent to: reviews@fullcirclemagazine.org
Questions for Q&A should go to: questions@fullcirclemagazine.org
Desktop screens should be emailed to: misc@fullcirclemagazine.org
... or you can visit our **site** via: fullcirclemagazine.org



FCM#156

Deadline:
Sunday 05th Apr. 2020.
Release:
Friday 27th Apr. 2020.



Full Circle Team



Editor - Ronnie Tucker
ronnie@fullcirclemagazine.org

Webmasters - Cees Rijken
and Chris Christensen
admin@fullcirclemagazine.org

Editing & Proofreading
Mike Kennedy, Gord Campbell, Robert Orsino, Josh Hertel, Bert Jerred, Jim Dyer and Emily Gonyer

Our thanks go to Canonical, the many translation teams around the world and **Thorsten Wilms** for the FCM logo.

Getting Full Circle Magazine:

For the Full Circle Weekly News:



You can keep up to date with the Weekly News using the RSS feed: <http://fullcirclemagazine.org/feed/podcast>



Or, if you're out and about, you can get the Weekly News via Stitcher Radio (Android/iOS/web):
<http://www.stitcher.com/s?fid=85347&refid=stpr>



and via TuneIn at: <http://tunein.com/radio/Full-Circle-Weekly-News-p855064/>



EPUB Format - Most editions have a link to the epub file on that issue's download page. If you have any problems with the epub file, email: mobile@fullcirclemagazine.org



Issuu - You can read Full Circle online via Issuu: <http://issuu.com/fullcirclemagazine>. Please share and rate FCM as it helps to spread the word about FCM and Ubuntu.

FCM PATREON: <https://www.patreon.com/fullcirclemagazine>