Oktobar—novembar 2015. **Broj 40**

LiBRE!

Časopis o slobodnom softveru

Tejls

JOŠ IZDVAJAMO

Bisajds konferencija u Beču

Kalibar — Virtualna biblioteka

Reč urednika

LiBRE! ide dalje

Najpre moramo da se zahvalimo svima koji su nam pisali i pružili nam podršku. Mnogima smo odgovorili na pismo i lično se zahvalili, a onim drugim, kojima nismo stigli da odgovorimo, izvinjavamo se i zahvaljujemo na ovaj način.

Uzevši u obzir količinu pisama i „lajkova" na društvenim mrežama, vrlo smo zadovoljni pruženom podrškom. Ruku na srce, nije to neki impozantan broj, tako da ćemo za sada morati da priznamo sebi da LiBRE! nije časopis koji revolucionarno menja svet i ustaljene navike. Za sada ćemo se zadovoljiti da smo plamičak koji gori i čeka pogodnije gorivo (bolje vreme i bolje ljude) koji će rasplamsati veću vatru.

Ovo podneblje Balkana je ranije u istoriji više živelo po filozofiji slobodnog softvera. Pružanje usluga prijatelju, seoske komšijske mobe bez novčane nadoknade su pravi ekvivalenti kako uglavnom funkcioniše razvoj slobodnog i besplatnog softvera otvorenog koda. Nikada nismo bili bogati, često smo bili porobljeni, a ipak smo se koliko-toliko razvijali. Naši dedovi su shvatali da sami ne mogu da urade ništa kapitalno. Zajedno sa rodbinom i komšijama je mnogo lakše. Pošto para nema, red je ako ti je neko pomogao da i ti pomažeš nekom drugom. Nekad vraćaš uslugu onom ko je tebi pomagao, ali to nije pravilo. Možeš da pomažeš i trećoj osobi koja će uslugu posle vratiti onome kome si ti dužan.

Da li je ovo najpravedniji sistem? Naravno da nije. Vrednost pruženih usluga nikada nije jednaka. Uvek neko daje više i to je uvek izvor nesuglasica. Zato su naši dedovi smislili poslovicu: „Čist račun, duga

ljubav”. U prevodu — ti platiš moju uslugu, a ja platim tvoju uslugu i svi su zadovoljni. To je dobro kad ima para, a kad ih nema, šta onda? Napreduje li samo onaj ko ima para?

Za siromašna društva kao što je naše bolje je voditi se poslovicom „u se i u svoje kljuse” i filozofijom slobodnog i besplatnog softvera otvorenog koda. Tom filozofijom će časopis dalje da funkcioniše. Svaki autor će pisati i deliti svoje znanje da bi i drugi tako radili, a kako bismo svi zajedno znali više. Glad za znanjem takođe može da bude dobra motivacija.

Dobili smo dosta korisnih sugestija i predloga koje ćemo probati da u narednom periodu, u skladu sa svojim stvarnim mogućnostima, primenimo i ispoštujemo. Ne možete od nas očekivati da na svaku temu znamo odgovor. Koliko znamo, toliko ćemo i pisati. To nije razlog da nam dalje ne pišete, ne kritikujete nas, ne hvalite nas i da ne zahtevate da pišemo o nekim vama značajnim temama. Ako znate nešto o slobodnom i besplatnom softveru otvorenog koda o čemu mi još nismo pisali i mislite da je značajno za ovu temu, slobodno nam ponudite vaš članak. On ne mora da bude idealno stilski napisan, imamo ljude koji to mogu da doteraju i pripreme za objavu. Naša adresa elektronske pošte je i dalje libre [et] lugons [dot] org.

Do sledećeg broja,

LiBRE! tim.

Sadržaj

Vesti str. 6

Puls slobode
Bisajds konferencija u Beču str. 10
Izveštaj sa BarKamp konferencije iz Banje Luke str. 14
Bitkoin — izveštaj sa trećeg sastanka str. 17

Predstavljamo
Sigurniji operativni sistemi (1. deo) — Tejls str. 20
Kalibar — Virtualna biblioteka str. 27

Kako da...?
Numerička obrada i simulacije str. 33

Slobodni profesionalac
P=NP problem str. 37

Server
Enkriptovanje i kopiranje servera korišćenjem Duplisiti programa str. 40

Mobilni kutak
F-Droid str. 44

Moć slobodnog softvera

Broj: 40
Periodika izlaženja: mesečnik

Izvršni urednik: Stefan Nožinić
Glavni lektor:
Admir Halilkanović

Lektura:
Jelena Munćan **Saška Spišjak**
Aleksandar Božinović
Aleksandra Ristović

Grafička obrada:
Dejan Maglov **Ivan Radeljić**

Dizajn: White Circle Creative Team

Autori u ovom broju:
Luka Hadži-Đokić **Petar Simović**
Nikola Todorović **Goran Mekić**
Nenad Marjanović

Ostali saradnici u ovom broju:
Marko Novaković **Mihajlo Bogdanović**

Počasni članovi redakcije:
Željko Popivoda **Željko Šarić**
Vladimir Popadić
Aleksandar Stanisavljević

Kontakt:
IRC: #floss-magazin na irc.freenode.net
E-pošta: libre@lugons.org
Veb: http:/libre.lugons.org

Vesti

29. septembar 2015.

Suosnivač Pajrat beja oslobođen zatvora

Gotfrid Svartholm je oslobođen zatvorske kazne od 3 godine.

Koristan link: http://j.mp/1P18Ysz

---

2. oktobar 2015.

Kalibre ima dobija podršku za KFIks

Ova alatka za upravljanje i prevođenje elektronskih knjiga iz jednog formata u drugi dobija podršku za KFIks (*KFX*) od Amazona.

Koristan link: http://j.mp/1NltYdp

---

14. oktobar 2015.

KDE puni 19 godina

„Popularnost Juniksa raste zahvaljujući slobodnim varijantama kao što je linuks. Ali još uvek nedostaje stabilno okruženje radne površi dobrog izgleda" - napisao je Matijas Etrih (*Matthias Ettrich*) 14. oktobra 1996. povodom objave svog novog projekta.

Koristan link: http://j.mp/1P195UP

---

21. oktobar 2015.

Francuska glasala za proširenje upotrebe slobodnog softvera

Francuska je na nacionalnom referendumu o digitalnim tehnologijama glasala za usvajanje predloga o proširenju upotrebe slobodnog softvera od strane vladinih organizacija i institucija.

Koristan link: http://j.mp/1QCwrjY]

---

22. oktobar 2015.

Digitalni potpisi na PDF datotekama stižu na Linuks

Popler projekat, koji koristi većina čitača elektronskih dokumenata na linuksu, dobija podršku za digitalni potpis i verifikaciju.

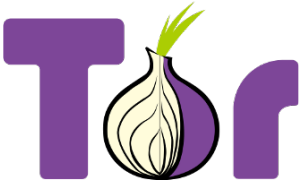
Koristan link: http://j.mp/1I8KN3w

---

29. oktobar 2015.

Tor ćaskanje

Tor projekat je objavio svoju aplikaciju za instant razmenu poruka preko ove mreže.



Koristan link: http://j.mp/1X75ngM

Vesti

31. oktobar 2015.

Epl objavio svoju biblioteku za kriptovanje

Ova kompanija je načinila slobodnim kod biblioteke koja služi za kriptografiju.

Koristan link: http://j.mp/1NltHal

---

10. novembar 2015.

Gugl objavio Tensorflou pod slobodnom licencom

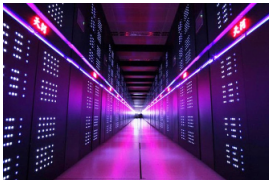
Gugl je objavio svoj alat za mašinsko učenje pod slobodnom licencom. Ovo će omogućiti bolju razmenu iskustva među istraživačima i lakšu implementaciju ovakvih aplikacija. Ovaj alat koriste ključni Guglovi servisi kao što je prevodilac i prepoznavanje govora. Ipak, nije objavljena puna verzija koja omogućava primenu na većim klasterima i mrežama računara.

Koristan link: http://j.mp/1kOPT0b

---

12. novembar 2015.

Lideri u industriji super-računara su se udružili u kreiranju novog frejmvorka



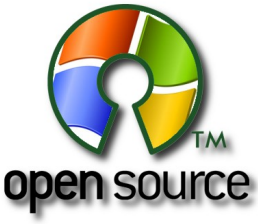
Linuks fondacija sa najvećim liderima u ovoj oblasti planira razvijanje frejmvorka otvorenog koda za HPC okruženje.

Koristan link: http://j.mp/1NltSIN

14. novembar 2015.

Majkrosoft je objavio svoju biblioteku za mašinsko učenje pod slobodnom licencom

Pored Gugla, i ova kompanija je objavila svoju biblioteku za mašinsko učenje pod MIT licencom. Za razliku od Gugla, ovaj skup alata omogućava upotrebu mašinskog učenja na distribuiranim sistemima.



Koristan link: http://j.mp/1lcTepl

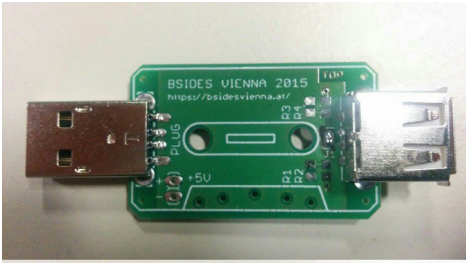
Bisajds konferencija u Beču

Autor: Goran Mekić

Od prijatelja iz Metalaba koji su ove godine bili na Balkonu (eng. *BalCCon*) čuli smo za Bisajds (eng. *BSides*). Iskreno, nismo znali šta da očekujemo, ali smo ipak odlučili da je digitalna sigurnost nešto što želimo da čujemo. I tako smo se zaputili u Beč da posetimo Bisajds i Metalab.

Odmah po ulazu nekoliko ogromnih iznenađenja:

- Ulaznica je USB kondom — malo parče elektronike koje vam omogućava da punite svoj telefon ili tablet preko USB-a na tuđim laptopima bez bojazni da mogu nešto da vam urade. Ideja je jednostavna — pošto u USB konektoru dva kontakta služe za napajanje a dva za podatke, oni za podatke nisu rutirani uopšte;



- Svaki posetilac je dobio majicu. Pošto se ulaznica ne plaća, ovo je veoma lep

gest od strane organizatora, te bismo iskoristili ovu priliku da im se zahvalimo;

- Organizatori su dobili budžet koji, dok se ne potroši, služi da bi posetioci dobili besplatnu kafu, čaj, sok i sendviče. Sve je učinjeno kako ne bismo morali napustiti prostorije;
- Ukoliko niste posetili zvanični sajt, preporučujemo da to uradite makar da biste videli „dizajn". Sve je u DOS maniru i imate osećaj da gledate u 386. Još više iznenađuje činjenica da gledate u Butstrap (eng. *Bootstrap*) temu;

Jedna loša vest u vezi s konferencijom je da organizator nije snimao predavanja. Ovo nam je bilo veoma čudno, ali uzevši u obzir da su neka od predavanja otkrila i neke tajne koje velike kompanije i vlade ne žele da objave, ne čudi odluka da predavači ostanu makar malo anonimni.

Od predavača o kojima definitivno smemo pisati ističe se Adrijan Dabrovski (*Adrian Dabrowski*) temom „Hakovanje Holivuda" u kojoj je ilustrovao neke od popularnih filmova i greške u hakovanju. Da budemo iskreni, nismo sigurni da li je prezentacija bila predavanje ili stendap komedija.

Drugo predavanje, koje nas je iznenadilo, prezentovao je Štefan Šumaher (*Stefan Schumacher*) pod nazivom „Psihologija bezbednosti". Štefan je iskusan bivši Net-Bi-Es-Di (eng. *NetBSD*) programer sa ogromnim znanjem psihologije i didaktike. Autor ovog teksta je imao sreću što je na predavanju pored njega sedeo pedagog pa je imao simultano prevođenje kako bi shvatio punu genijalnost Štefanovog predavanja. Da ne bude zabune, Štefanovo znanje engleskog je perfektno, ali znanje iz psihologije autora ovog teksta je blizu nule, pa je prevod bio potreban kako bi razumeo neke od termina koje je koristio (prim.aut.).

Jedno od naprednijih predavanja je bila „Studija slučaja o sigurnosti upravljanja aplikacija prema beloj listi"[1] koje je držao Rene Frajngruber (*René Freingruber*). Pošto ova metoda postaje sve popularnija u velikim kompanijama, ova tema postaje i tek će postati zanimljiva, pošto je Rene efikasno pokazao kako obići zabrane kako kroz Vižual Bejzik Skript, tako i kroz Paueršel (*PowerShell*). Za one koji vole da se spuste veoma nisko na nivo asemblera i memorijskih lokacija,

[1] *Case study on the security of application whitelisting*; Bela lista je lista na koju se dodaju aplikacije koje steknu korisničku dozvolu. Samo aplikacije sa liste se mogu pokrenuti.

pokazao je šta se tačno dešava i na tim nivoima.

Možda i najveće iznenađenje bio je škotski haker Majkl Džek (*Michael Jack*). Šok za mnoge može biti izbor studijskog programa na kojem je Majkl već drugu godinu — etičko hakovanje. Nikada nismo čuli da ijedan fakultet u Evropi pruža i ovu vrstu obrazovanja (prim aut.). Iznenađenje je bilo to što je Majkl došao kao posetilac, da bi nakon otkazivanja jednog predavača uskočio i održao predavanje „Kripto ratovi 2" (*Crypto Wars 2.0*). Majkl je ili veoma iskusan predavač ili prirodni talenat, pošto je pažnju svih nas držao od početka do kraja sa zamalo otvorenim ustima. Predavanje je prikazalo razvoj kriptografije kroz istoriju, ključne igrače (kako pojedince tako i organizacije), algoritme koji su korišćeni i ko ih je implementirao, te uticaj organizacija kao što su američka Agencija za nacionalnu bezbednost (*NSA*) i britanski Štab za komunikacije (*GCHQ*) na oslabljivanje algoritama enkripcije sa citatima o kriptografiji ličnosti kao što su aktuelni premijer Britanije Dejvid Kamerun (*David Cameroon*). Zbog ovakvih citata ni za Majkla nismo sigurni da li je držao predavanje ili stendap komediju.

Za pun spisak predavanja posetite http://bsidesvienna.at/talks/. Obećavamo da se nećete pokajati.

Nakon konferencije druženje je nastavljeno u bečkom hakerspejsu koji se zove Metalab, o čemu ćemo pisati u sledećem broju.

Puls slobode

Izveštaj sa BarKamp konferencije iz Banje Luke

Autor: Goran Mekić

Počevši od tema, drugi banjalučki BarKamp je oduševio, ako nikog drugog, onda autora ovog teksta. Govoreći slengom programera, teme su bile izuzetno „niskog nivoa”[1] — od kernel programiranja, preko iskorišćenja slabosti programa za dobijanje prava korenskog korisnika (rut) do korupcije podataka na medijumima usled različitih događaja kao što su pisanje u memorijsku lokaciju blizu one koju želimo da promenimo, kosmičkih zraka, kvantnih fluktuacija i svih onih bizarnih i čudnih situacija koje niko ne može objasniti. Ruku na srce, bilo je i malo manje „niskih“ predavanja, kao što su „Kako postati frilenser i kako opstati kao frilenser” i veb programiranje uz Flask i Pajton. Uzevši u obzir izbor tema i njihovu težinu, veoma iznenađuje pažnja publike koja je u skoro nepromenjenom broju ispratila događaj do samog kraja.

[1] U slengu, površinski nivo označava sve što se pokreće na operativnom sistemu. S druge strane, niski (duboki) nivo se najčešće odnosi na komponente sistema, na kernel i na upravljačke programe. .

Pa da krenemo od početka. Samo pet sati puta nas je delilo od apsolutne zabave uz hakere. Uz carine, tričavih sedam sati je prošlo u društvu brže nego što smo očekivali. Sutradan je na ETF-u počelo dešavanje, radi kojeg smo svi došli, uz manje probleme sa mrežom. Na prvom predavanju se videlo da se ekipa predavača ne šali kada su teme u pitanju. Dragan Simić je pričao šta je to tzv. efekat „čekićanja vrste" (eng. *row hammer*, prim.prev.) ili kako izmeniti bit u memoriji kom nemamo pristup. Ukratko, zbog gustine bitova na fizičkim čipovima, električni naboj koji predstavlja bitove ponekad može da „procuri" na susednu lokaciju. Dragan je predstavio šta su istraživači radili da spreče ovakvo ponašanje memorije kroz softver i hardver. Isti predavač je kasnije pričao i o tome kako se bitovi na medijumima ponekad promene iako im niko nikad nije pristupao. Iako se ovo statistički retko dešava, postoje slučajevi u kojima to nije zanemarljivo. Kao primer dat je VHS i da od nekoliko desetina petabajta, *128MB* podataka bude korumpirano bez mogućnosti ispravke.

Nikola Nenadić je pričao o dvema veoma interesantnim temama u vezi sa kernelom: pisanje drajvera (upravljačkih programa) i korišćenje kompresije memorije u kernelu (*zram*, *zswap* i *zcache*). Interesantna činjenica je da, iako računar veoma dobro radi sa brojevima sa pokretnim zarezom, u kernelu je zabranjeno koristiti ih. Sa druge strane, ukoliko imate stari hardver sa malo memorije, kompresovanje podataka pre snimanja u memoriju može da vam oživi taj hardver.

Puls slobode

Autoru najzanimljivije predavanje je bilo o bagovima korupcije memorije koje je držao Strahinja Piperac. Veoma lepo je objasnio šta su to sigurnosni propusti na niskom nivou: prelivanje bafera (eng. *buffer overflow*), bagovi u formatiranju stringova (eng. *format string attack*), izlazak van opsega intidžera (eng. *integer overflow*) i drugi. Takođe, prikazao je nekoliko tehnika zaštite koje su implementirane, objasnio je zašto je nemoguće zaštititi se nekom alatkom koja bi automatski odbijala napade i prikazao zašto je uopšte nemoguće braniti se od napada bilo čime što nije dobro programiranje.

Autor ovog teksta je pričao o veb razvoju uz Flask razvojni okvir (eng. *Flask framework*) i Pajton jezik. Predavanje je bilo na početnom nivou i cilj je bio izneti ideje koje se ne nalaze u drugim rešenjima. Takođe, prisutni su mogli čuti kako od Flaska, koji je po dizajnu minimalan, napraviti korisno razvojno okruženje uključivanjem proširenja.

Za kraj, Goran Jakovljević je pričao kako postati frilenser, šta su najčešće greške, kako najbrže doći do posla i zadržati klijente.

Sve one koji nisu bili u mogućnosti da prisustvuju možemo obradovati vešću da je organizator obećao da će sva predavanja biti okačena na Jutjub kanal kada se završi montiranje.

Bitkoin — izveštaj sa trećeg sastanka

Autor: Aleksandar Božinović

Treći sastanak beogradske grupe okupljene oko bitkoina održao se 30. oktobra 2015. godine u beogradskom haklabu u Daničarevoj ulici, broj 23, sa početkom u 18 časova. Glavna tema sastanka bila je Bitkoin tehnologija — šta nam ona donosi, koje su to nove inovacije i kolika je upotreba Bitkoina u svetu. Podsećanja radi, bitkoin je kripto-valuta, digitalni novac. Organizator trećeg sastanka je član beogradskog haklaba Petar Simović, ujedno i autor u LiBRE! časopisu. Inicijator prvog okupljanja je bio izvesni Dušan na sajtu http://www.meetup.com/Beograd-Bitcoin-Meetup/. Na sastanku je bilo jedanaest ljudi, što je pomak u odnosu na drugi put kada se sastalo osam ljudi. Zanimljivo je spomenuti da je među njima bilo studenata i srednjoškolaca. Sastanci se uglavnom organizuju jednom mesečno. Smatraju da je to dovoljno da bi se stekle nove teme za razgovor. Po rečima Petra, ljudi koji dolaze na sastanke znaju iznenađujuće mnogo o Bitkoinu. Međutim, to se ne odnosi toliko na tehnički deo, koliko na praćenje dešavanja vezana za bitkoin u svetu.

Na prethodno spomenutom sajtu organizator navodi da će novi članovi dobiti bitkoine u vrednosti od 10 dinara. Bitkoini se poklanjaju da bi se početnici

podstakli da naprave novčanike za primanje novca i time se neposredno upoznaju sa ovom tehnologijom na praktičan način. Ovaj potez nam „suvu teoriju" pretače u stvarnost i pokazuje nam koliko jednostavno i praktično može biti korišćenje bitkoina i bez prevelikog znanja i razumevanja kriptografije, ekonomije i računarskih mreža. Iako na trećem sastanku nije prikazana transakcija, to se moglo videti na prethodnim sastancima, a svi zainteresovani moći će to da vide na budućim sastancima. Na sastanku se moglo čuti da se bitkoin može koristiti i kao sredstvo plaćanja u jednom kafiću u Beogradu. Radi se o kafiću „Apetit" (*Appetite*, Kraljice Natalije br. 30) u kojem postoji bankomat koji menja dinare u bitkoine. Postoji ideja da se neki naredni sastanak održi upravo tamo.

Beogradski haklab je mesto prilagođeno za vršnjačku edukaciju. Kao takvo, vrlo je pogodno i za okupljanja ovog tipa, sve dok broj ne prelazi dvadeset, po slobodnoj proceni autora ovog teksta. Sve vreme je vladala prijatna atmosfera, a Petar, domaćin haklaba, postarao se da svi budu posluženi čajem, sokom i slatkišima. Mnogi učesnici su na sastanak doneli svoje laptope i telefone, a ko nije do tad imao svoj virtuelni novčanik, mogao ga je ovom prilikom steći, a zatim i dobiti pokoji bitkoin na poklon. Duh slobode utisnut je u stikere koji su nalepljeni na gornju stranu većine laptopa prisutnog osoblja. To su stikeri sa logoom Ubuntua, Fedore, zatim logo omražene Američke bezbednosne agencije, Tora i Fajerfoksa. Jedan laptop krasio je stiker sa Balkona (videti prethodna dva broja).

Na sastanku se diskutovalo o koristi tzv. „rudarenja" (eng. *mining* — specifični proces generisanja novih bitkoina). Jedan od zaključaka bio je da najveću korist mogu steći oni koji imaju specijalnu napravu zvanu „asik" (eng. *asic — application-specific integrated*

circuit), dok pojedinci koji koriste svoje računare bez dodatne opreme, sem entuzijazma, preterane vajde nemaju.

Veoma zanimljiva vest koja se na sastanku mogla čuti je da je u Rusiji napisan nacrt zakona prema kojem se zabranjuje bitkoin i koji, naime, preti zatvorskom kaznom u trajanju do četiri godine. Rusija pokušava na ovaj način da zaštiti svoju valutu. Više o tome na http://izvestia.ru/news/593841 .

Rasprava se povela i u smeru pravne zaštite lica od kojih je bitkoin ukraden. Glavno pitanje je, da li bi državni organi (npr. policija i sudstvo) mogli da prepoznaju krađu bitkoina kao pravu krađu, odnosno kao krivično delo? Pošto je bitkoin zasnovan na otvorenom kodu, spomenute su tzv. kripto-valute koje su nastale na sličnom principu po kojem je bitkoin razvijen (naprimer tzv. Deš — eng. *Dash*). Moglo se čuti poređenje pojedinih kripto-valuta, a učesnici rasprave postavili su hipotetički model nove kripto-valute i uspostavili su njene osnovne principe. Učesnici su jednoglasno saglasni sa tim da se velika prednost bitkoina ogleda u tome da se za pojedinu transakciju plaća svega 0.000113 bitkoina (trenutno 4 dinara) bez obzira na iznos koji se prenosi, u odnosu na konvencionalne načine transfera novca za šta banke „debelo" naplaćuju svoje usluge.

Ukoliko vas ova tema interesuje i želite da sa ostalima diskutujete o bitkoinu, možete se priključiti grupi http://www.meetup.com/Beograd-Bitcoin-Meetup/. Dobar razgovor i prijatna atmosfera su zagarantovani.

Predstavljamo

Sigurniji operativni sistemi — (1. deo)

Autor: Petar Simović

Svakako da danas više vodimo računa o sopstvenoj privatnosti kako na internetu na društvenim mrežama tako i lokalno na svom računaru. Naravno da je stalno potrebno paziti na koje linkove klikćemo na internetu, kakve fajlove otvaramo u elektronskoj pošti, koje programe pokrećemo na našem računaru i sa kojim pravima izvršavanja. To bi trebalo da bude rutina svakog odgovornog korisnika, a ne paranoično ponašanje. Pošto smo već kod onih malo nepoverljivih i opravdano paranoičnih korisnika, vreme je da predstavimo Tejls (eng. *TAILS*, *The Amnestic Incognito Live System*), za kojeg su verovatno mnogi čuli, a možda ga i isprobali, ili ga odavno koriste.

Tejls je baziran na Debijanu (eng. *Debian*), pokreće se u živom modu (eng. live mode), što znači da neće pristupati hard disku vašeg računara, već samo radnoj ili glavnoj memoriji. Obično se narezuje na neki spoljnji medijum kao što su DVD i USB, sa kojeg se pokreće pri startovanju računara. U ovom opisu nećemo proći kroz proces pravljenja butabilnog USB-a ili DVD-a, ali ćemo uputiti na neophodan softver kojim to možete uraditi. Takođe, detaljno ćemo objasniti primenu ovog operativnog sistema, kao i softver kojim je opremljen.

Pre svega nam je potreban sam operativni sistem koji dolazi u podrazumevanom **.iso** formatu, a može se preuzeti sa strane Tejls projekta: https://goo.gl/uRzSD7.

Kada imamo **.iso** sliku sistema, najpre bi trebalo da proverimo autentičnost i verodostojnost preuzetog **.iso** fajla, to jest da se uverimo da fajl nije presretnut negde na mreži, menjan, kao i da je baš od onoga od koga bi trebalo da bude. Ovo nije neophodno, ali se toplo preporučuje zbog mogućeg tzv. „čoveka u sredini" (eng. *Man In The Middle*, ili najčešće skraćeno *MiTM*). Da bismo to uradili, potrebno je da preuzmemo i digitalni potpis **.iso** slike, kao i da u gpg (eng. *Gnu Privacy Guard*) ubacimo javni ključ Tejlsovog razvojnog tima, koji garantuju svojim digitalnim potpisom za sistem. Javni ključ možete preuzeti sa https://tails.boum.org/tails-signing.key i ubaciti ga u gpg izvršavanjem komande:

```
gpg --keyid-format long --import tails-signing.key
```

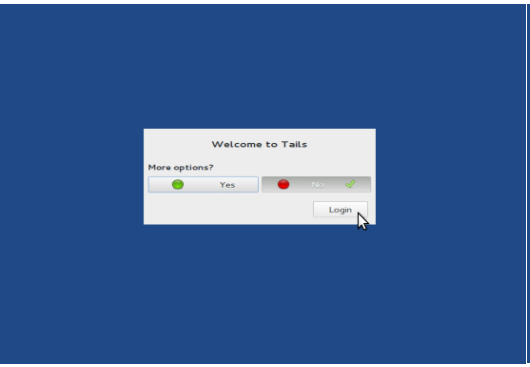
Potom je potrebno preuzeti i digitalni potpis sa https://goo.gl/YpoVOU (ovaj potpis važi samo za verziju 1.7) i sačuvati ga u folderu gde je i **.iso** slika. U trenutku pisanja ovog teksta najnovija verzija je 1.7, pa je komanda koja se izvršava iz foldera gde su digitalni potpis i slika sledeća:

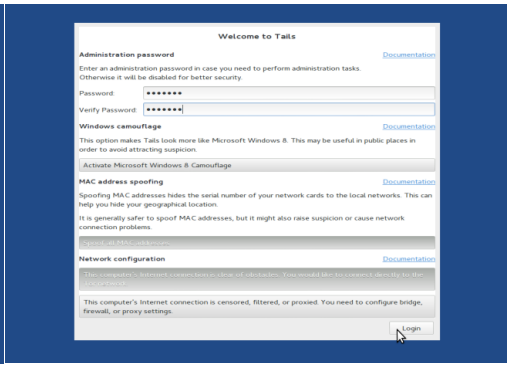
```
gpg --keyid-format 0xlong --verify tails-i386-1.7.iso.sig tails-
i386-1.7.iso
```

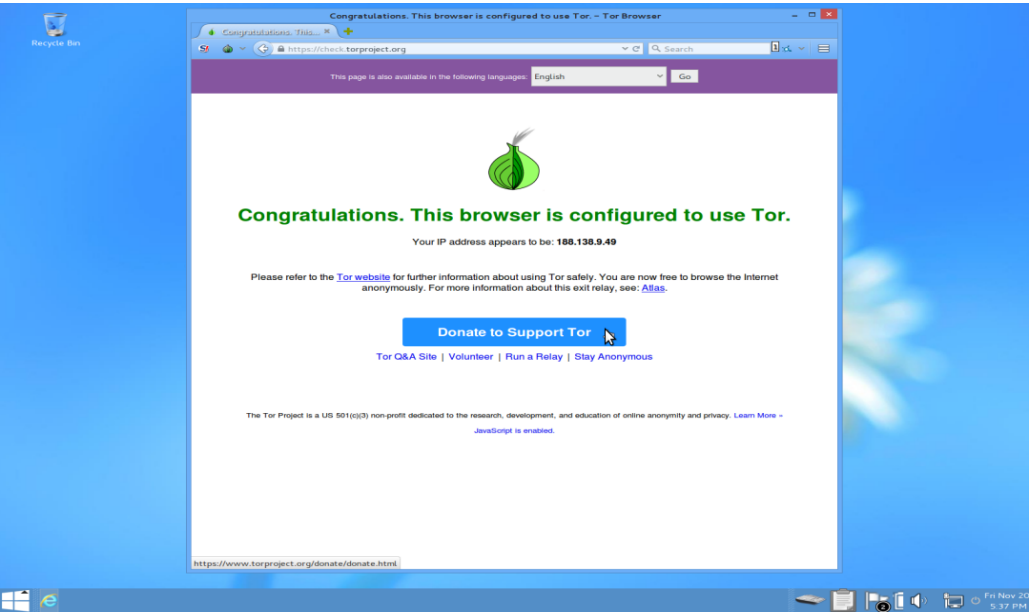
Prvi način je da sistem pokrenemo iz virtuelne mašine korišćenjem Virtuelboksa (eng. *Virtualbox*, https://goo.gl/rwxEO8), dok je drugi metod sa živim operativnim sistemom na spoljašnjem medijumu praktičniji i prenosiviji. Pa ukoliko koristite USB, trebate program za pravljenje žive distribucije na njemu, a to su Junetbutin (eng. *Unetbootin*, https://unetbootin.github.io/) i Jumi (eng. *Yumi*, http://goo.gl/8pnNww), dok je u slučaju narezivanja sistema na CD i DVD podrazumevani program na vašem linuksu poput Brazera i Iksefberna (eng. Xfburn) dovoljan.

Nakon startovanja Tejlsa, pri prikazivanju plavog grafičkog korisničkog interfejsa, treba da odaberete da li želite još opcija ili ne. Za početnike koji samo žele da koriste osnovne programe koje Tejls pruža, odgovorite sa **ne**. Ali ukoliko želite ili imate potrebu da promenite vašu mak (eng. *MAC*) adresu kako bi bilo teže da vas identifikuju po uređaju koji koristi mrežu, ili želite da zamaskirate Tejls da izgleda kao da je Vindouz osam (eng. *Windows 8*) operativni sistem na mreži i tako se lakše stopi u okolinu ne privlačeći neželjenu pažnju na mreži koju koristite, ili je prosto zabranjen pristup Tor mreži, pa morate da koristite tzv. Tor mostove (eng. *Tor bridges*) – onda je potrebno da odaberete opciju **da** (eng. *Yes*)

i tu konfigurišete ove tri opcije u skladu sa vašom situacijom.



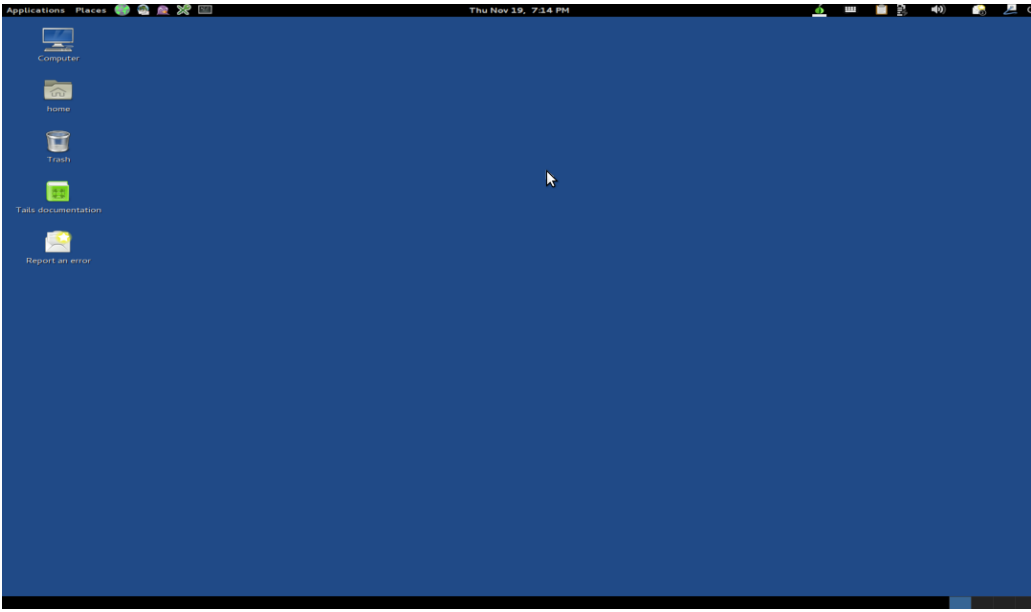




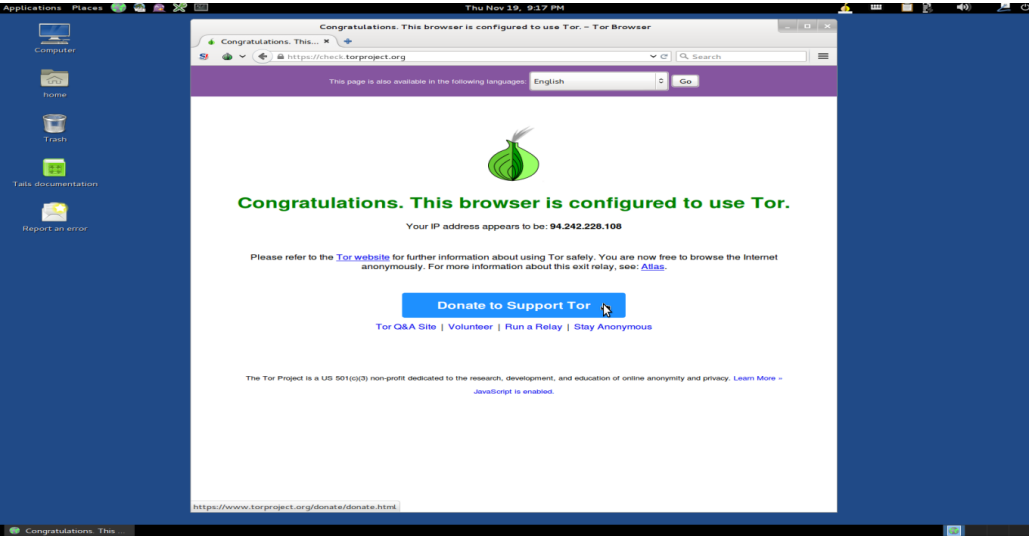
Nakon toga imate funkcionalno okruženje. Zatim je potrebno da se povežete na mrežu i sačekate da se automatski pokrene Tor i da se pojavi obaveštenje da je Tor spreman za korišćenje. Ovo je bitno jer je ceo operativni sistem napravljen

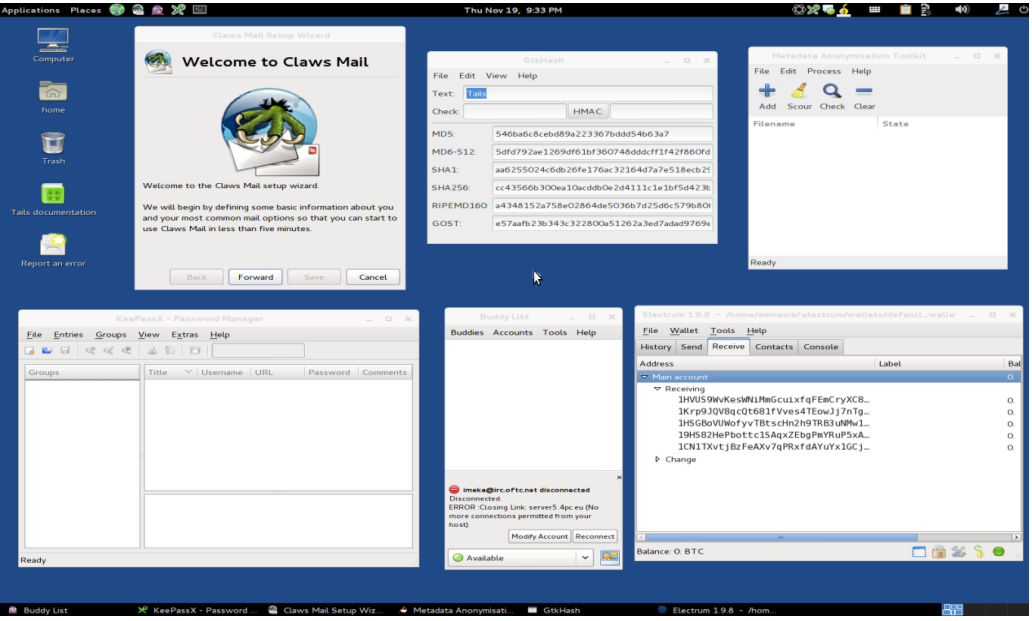
oko ideje o lakom korišćenju Tor mreže. Svi programi koji koriste mrežu su podešeni da koriste Tor kako bi korisnik ostao anoniman i na taj način mu obezbedio privatnost, dok će programi koji pokušavaju da izađu na mrežu bez Tora biti prekinuti radi bezbednosti. Više možete pročitati na samom sajtu projekta: https://goo.gl/jDt1X. Samo da podsetimo čitaoce da smo Tor mrežu detaljnije opisivali u tri broja LiBRE! časopisa (22, 23. i 24).

Osnovni programi su Pidžin, kojeg smo u prethodnom broju opisali, Kloz mejl klijent (eng. *Claws mail*), Ki-pas-iks (eng. *KeePassX*) menadžer za čuvanje svih vaših naloga pod jednom šifrom, kao i neizostavni Tor internetski pregledač (eng. *Tor Browser Bundle*). To su samo programi koji se vide sa radne površi, ali, naravno, ima ih još. Izdvojićemo svakako MAT (eng. *Metadata Anonymisation Toolkit*), alat za brisanje metapodataka, opisan u broju 26, Elektrum (eng. *Electrum*), prenosivi novčanik za anonimnu digitalnu kripto-valutu — bitkoin (eng. *Bitcoin*), o kojoj će biti više reči u nekom od narednih brojeva.



Predstavljamo





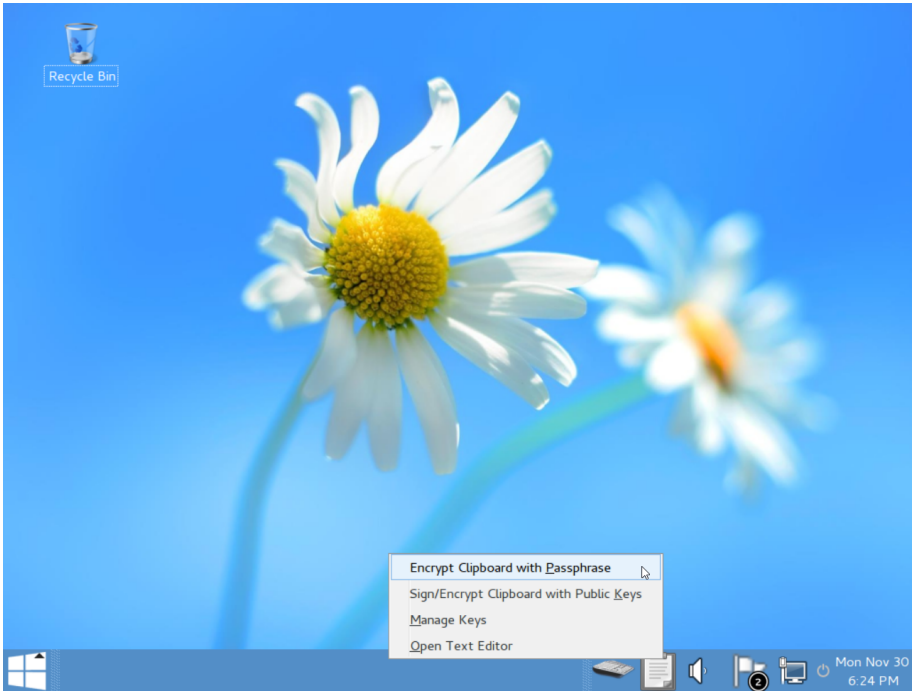
Pored sigurnosnih, tu je i ceo Libreofis paket, kao i programi za grafičku obradu:

- Gimp,
- Inkskejp (eng. *Inkscape*),
- Skribus (eng. *Scribus*).

Što se tiče programa za obradu, uređivanje, snimanje zvuka i video materijala, tu su:

- Odasiti (eng. *Audacity*),
- Traverso,
- Pitivi i drugi.

Međutim, još je interesantnije to da se Tejls može instalirati (ne narezati) na fleš memoriju i pri tom šifrovati sve podatke datotečnog sistema fleš memorije na koju se instalira (eng. *persistance*, https://goo.gl/yzwES0), osim nekoliko neophodnih za pokretanje sistema. To znači da možete da čuvate podatke unutar Tejlsa i nakon što ugasite računar, za razliku od opcije živog operativnog sistema, koji će obrisati sav RAM po gašenju ili restartovanju. Ovo brisanje RAM-a je korisno jer sprečava takozvani „napad hladnog startovanja" (eng. *cold boot attack*, Vikipedija: https://goo.gl/AUUbUP), jer RAM čuva sadržaj i do minut ili dva posle gašenja računara, a uz pomoć malo kompresovanog vazduha memorija se može momentalno zamrznuti i time znatno produžiti vreme čuvanja podataka u RAM-u. Podsećamo da se u RAM-u mogu nalaziti razni enkripcioni ključevi, pa je ovo svojstvo veoma korisno. Pored brisanja RAM-a pri gašenju ili restartovanju, Tejls ima i opciju da šifrujete klipbord (eng. *clipboard*), to jest onaj deo memorije u koji se sprema sadržaj kada kliknete na opciju za kopiranje (eng. *copy*).



Za kraj, važno je reći da je Tejls dizajniran za najkritičnije slučajeve kada su korisnici čak i u neposrednoj životnoj opasnosti ukoliko njihov identitet bude otkriven. Od dna pa do vrha sistem je dizajniran i osmišljen sa digitalnom sigurnošću i privatnošću na umu, jer je namenjen za uzbunjivače, novinare, aktiviste i sve one kojima su neophodni anonimnost i privatnost za posao kojim se bave u uslovima represivnih režima država u kojima borave. Kao primer bismo naveli Edvarda Snoudena (eng. *Edward Joseph Snowden*), kome je Tejls svakako dosta pomogao da pobegne i prosledi poverljive dokumente novinarima. Ali ne samo za ljude sa opasnim poslom, sistem je namenjen za sve obične korisnike koji žele da iskoriste svoje pravo na privatnost među računarskim mrežama.

Kalibar

Virtualna biblioteka

Autor: Dejan Maglov

Predstavljamo vam ovog puta softver koji je namenjen ljubiteljima pisane reči. Kalibar (eng. *Calibre*) je sveobuhvatno rešenje za upravljanje i održavanje virtualne biblioteke elektronskih knjiga. Kada kažemo „sveobuhvatno rešenje", mislimo na to da Kalibar nije samo čitač elektronskih knjiga nego mnogo više od toga, ali idemo redom.

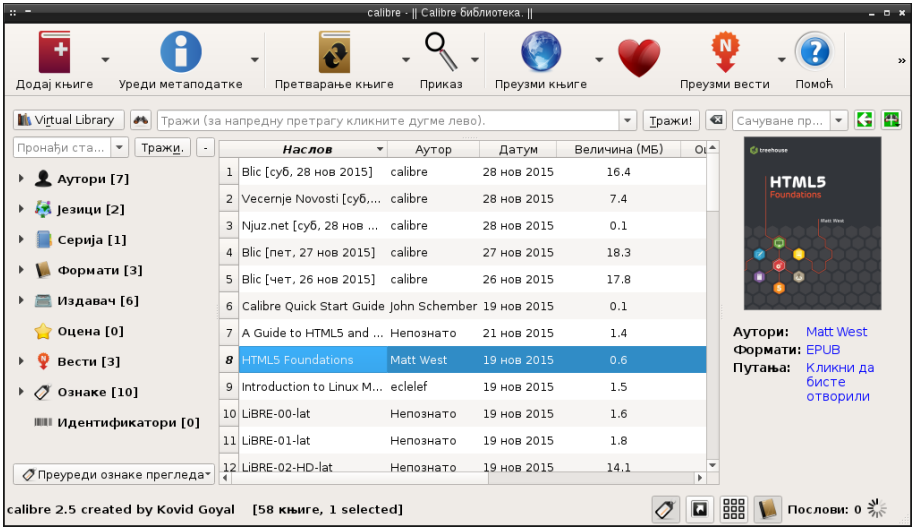
Istorija

Na primeru razvoja Kalibra možemo još jednom da pokažemo uspešan način razvoja slobodnog softvera.

Sve je počelo 2006. godine kada je autor ovog projekta, Kovid Gojal, uočio da Sonijev PRS-500, komercijalni čitač elektronskih publikacija, ne radi na linuksu. Obrnutim inžinjeringom uspeo je da razvije **Libprs500** što predstavlja preteču Kalibra.

Sledeći korak u razvoju Kalibra je dodavanje funkcije konvertora koji je vršio pretvaranje drugih formata elektronskih knjiga u LRF, format za Sonijev PRS-500 čitač.

Tu autor Kalibra nije stao. Vremenom je sakupio priličnu kolekciju elektronskih publikacija i zatrebala mu je organizacija tih publikacija. U tu svrhu je **Libprs500** dobio grafički interfejs i menadžera kolekcije publikacija (virtualnu biblioteku). Tada je ovaj program konačno dobio ime koje nosi i danas.



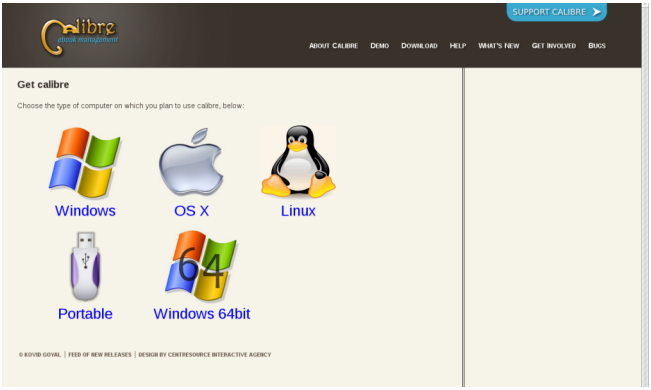
Ovako upakovan, Kalibar je privukao zajednicu slobodnog softvera da se pridruži u daljem razvoju projekta. Danas Kalibar ima desetine programera, testera, volontera za prevođenje i prijavljivača grešaka (bagova). Kontinuirano se razvija i dobija sve više novih funkcija.

Instalacija

Kalibar je multiplatformski softver. Na internetskoj stranici projekta (http://calibre-ebook.com/download) mogu se naći pripremljeni binarni paketi za instalaciju za Vindouz (32-bitnu i 64-bitnu verziju), Mek OS 10, kao i portabilna verzija namenjena instalaciji na prenosnim USB diskovima.

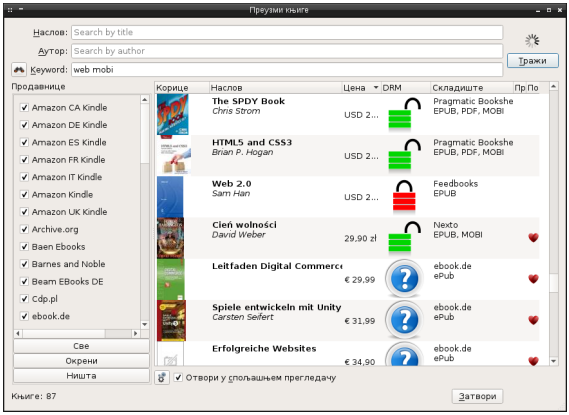
Kalibar se uglavnom ne nalazi u standardnom paketu predinstaliranih programa na GNU-Linuks sistemima. Bez obzira na to, sve GNU-Linuks distribucije u svojim riznicama uglavnom imaju pripremljene binarne pakete za instalaciju Kalibra. Ukoliko to ipak nije slučaj sa vašom distribucijom, možete ispratiti uputstvo za instalaciju sa već pomenute internetske stranice projekta.

Kalibar je prilično složen skup softvera koji zahteva dosta međuzavisnosti pa se ne preporučuje instalacija iz izvornog koda iako i ta mogućnost postoji.

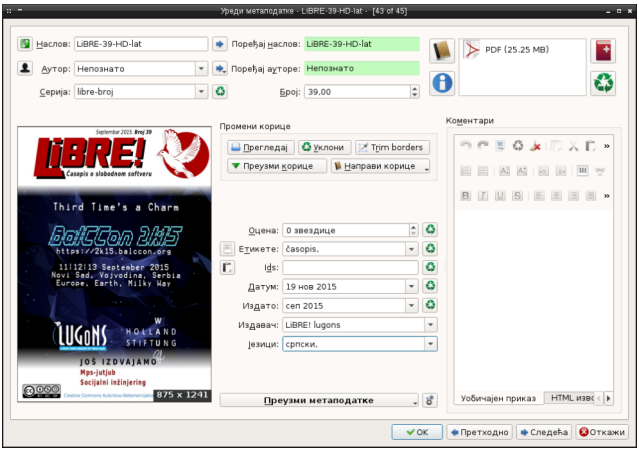


Kućna virtualna biblioteka

Kalibar je prvenstveno menadžer biblioteke elektronskih publikacija. Prepoznaje sve do sada poznate formate elektronskih publikacija, njih ukupno dvadeset sedam (*AZW, AZW3, AZW4, CBZ, CBR, CBC, CHM, DJVU, DOCX, EPUB, FB2, HTML, HTMLZ, LIT, LRF, MOBI, ODT, PDF, PRC, PDB, PML, RB, RTF, SNB, TCR, TXT* i *TXTZ*). Autori Kalibra su se potrudili da dodavanje knjiga u biblioteku dovedu do savršenstva. Knjige je moguće priključiti biblioteci iz svih lokalnih izvora (lokalnih tvrdih diskova, prenosnih medija i uređaja, direktorijuma, direktorijuma sa poddirektorijumima i tako dalje). Osim ovog načina, moguće je koristiti mrežne izvore, lokalne mreže ili internetske lokacije (prodavnice), pretragom za novim naslovima po naslovu, autoru ili ključnoj reči.

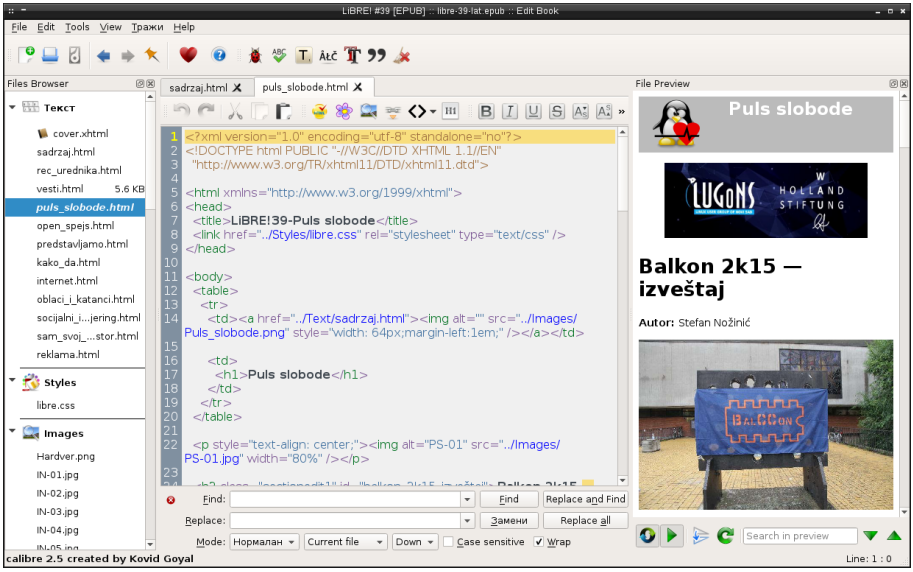


Manipulacija i sortiranje publikacija su takođe dovedeni do savršenstva. Uređivanjem metapodataka o svakoj publikaciji moguća je laka pretraga i pronalaženje željene publikacije u veoma velikim kolekcijama. Da se podsetimo, metapodaci su propratne informacije o nečemu, a publikacije prate informacije o naslovu, autoru, serijalu, broju, oceni, kategoriji, identifikatoru, datumu unosa u biblioteku, datumu izdavanja, izdavaču, jeziku, komentaru i formatu.



Uređivanje biblioteke publikacija raznih formata ne bi imalo smisla kada svaki od uvezenih formata ne bi bilo moguće otvoriti u odgovarajućem čitaču. Kalibar se sjajno snalazi sa svim formatima. Većinu formata otvara u sopstvenom čitaču elektronskih knjiga, ali isto tako sarađuje sa drugim eksternim čitačima poput podrazumevanog PDF čitača.

Kalibar podržava veliki broj uređaja za čitanje elektronskih knjiga sa kojima sinhronizuje kolekcije publikacija. U tu svrhu se koristi i njegov konvertor formata. Konvertor podržava devetnaest izlaznih formata (*AZW3*, *EPUB*, *DOCX*, *FB2*, *HTMLZ*, *OEB*, *LIT*, *LRF*, *MOBI*, *PDB*, *PMLZ*, *RB*, *PDF*, *RTF*, *SNB*, *TCR*, *TXT*, *TXTZ* i *ZIP*). Konvertovanje nije uvek idealno. Naročito je problematično konvertovanje PDF formata u druge formate zbog njegove složenosti.



To što konvertor ne odradi idealno moguće je popraviti u ugrađenom editoru. Ovaj editor je sasvim solidan i može da se, osim ispravki, koristi i za kreiranje nove elektronske publikacije. Upoređujući ga sa Sidžilom, malo je lošiji. Sidžil nudi malo više pomoći autoru. Treba takođe napomenuti da je ovaj editor kompatibilan samo sa **AZW3** i **EPUB** formatom. Ostale formate morate konvertovati u ova dva formata pre uređivanja, a nakon uređivanja ponovo vratiti u željeni format sa nadom da se nešto neće opet istumbati.

Zaključak

Svedoci smo popularnosti mobilnih uređaja i da sve više izdavača, čak i kod nas, ravnopravno nudi elektronska izdanja svojih knjiga uporedo sa papirnatim

izdanjima i to po povoljnijim cenama u odnosu na papirnata izdanja. Naročito se to moglo videti na poslednjem sajmu knjiga u Beogradu. Ova činjenica daje još veći značaj čitačima elektronskih izdanja.

Kalibar je ozbiljno parče softvera koji rešava sve probleme u vezi sa organizacijom — sakupljanje, čitanje, uređivanje i kreiranje elektronskih publikacija. Sa velikom sigurnošću možemo da tvrdimo da je Kalibar najkvalitetniji softver ove namene ne samo na linuksu nego i na drugim operativnim sistemima.

Kalibar je namenjen ravnopravno čitaocima, kolekcionarima i autorima. Svi oni će naći svoju primenu ovog softvera.

Pregled popularnosti GNU-Linuks i *BSD* distribucija za mesec novembar

Distrowatch

1	Mint	3336>
2	Debian	1885>
3	openSUSE	1873<
4	Ubuntu	1447<
5	Fedora	1387<
6	Mageia	1100>
7	Manjaro	993<
8	CentOS	835<
9	Kali	788<
10	Puppy	774>
11	Arch	771<
12	Netrunner	695>
13	Android-x86	663>
14	Zorin	658<
15	PCLinuxOS	600<
16	antiX	589>
17	LXLE	539<
18	Lubuntu	509<
19	ClearOS	505=
20	Chakra	503>
21	KNOPPIX	502>
22	Ubuntu MATE	494<
23	Black Lab	470<
24	Bodhi	462>
25	Chromixium	439<

Pad <
Porast >
Isti rejting =
(Korišćeni podatci sa Distrovoča)

Numerička obrada i simulacije

Autor: Stefan Nožinić

Samom pojavom računara nastala je mogućnost brzog izvršavanja velikog broja operacija. To znači da se omogućilo brzo rešavanje raznih jednačina i sličnih problema i na taj način su se mnogi problemi u prirodnim ali i društvenim naukama mogli brzo rešiti. To je brzo postalo popularno, postalo je jedna od glavnih primena računara, pa se izdvojilo kao zasebna oblast računarstva. Ta oblast se bavi raznim metodama za izračunavanje i simulaciju raznih fizičkih sistema, brzu obradu podataka i brzu vizualizaciju podataka. Ovo je omogućilo donošenje važnih zaključaka u vezi sa ponašanjem pojedinih sistema u određenim uslovima. Treba naglasiti da su ti sistemi uglavnom haotični i da se ne mogu rešiti analitički kako je to rađeno pre pojave računara i metoda za numerička izračunavanja.

Dok se skoro celo računarstvo bazira na činjenici da se operacije vrše u diskretnom domenu, ova oblast računarstva koristi kontinualne vrednosti kao što su vreme, pritisak i distanca. Iako se numerički metodi oslanjaju na kontinualne vrednosti i promenljive, ne smemo zaboraviti da računari i dalje imaju samo operacije za rad sa diskretnim vrednostima koje se „vrte ispod haube". Zbog ovoga dolazi do gubitka tačnosti i, ako je sistem takav, može da pokaže neželjeno ponašanje. Pored ovog problema, ne smemo zaboraviti da izračunavanje može biti veoma sporo ako je broj trivijalnih računarskih operacija previše veliki. Između ova dva zahteva često treba pronaći kompromis jer veća tačnost zahteva i više operacija što dodatno usporava ukupno vreme izračunavanja. Takođe, računari su ograničeni i radnom memorijom čije zauzeće raste kada se i sami podaci za obradu povećaju.

Dok standardni računarski algoritmi koji rade sa diskretnim vrednostima imaju problem sa vremenom i memorijom, numerički algoritmi imaju i dodatni problem: tačnost rezultata.

Pored svega ovoga, numerički metodi imaju veliku primenu u današnje vreme — od kućnih računara, video igrica pa sve do predviđanja vremenskih uslova i svemirskih istraživanja i izrade opreme za te namene. Ovo je nateralo naučnike da se pozabave ključnim problemima koji se nameću prilikom numeričke obrade podataka i simulacije sistema.

Skoro svaki problem u numerici se može svesti na jednostavniji problem koji ima slično rešenje ili praktično približno isto kao očekivano rešenje. Ovaj proces se može videti kroz mnoge primere, a neki od njih su:

- Beskonačan broj iteracija se može zameniti konačnim brojem sve dok rešenje ne postane dovoljno blisko željenom;
- Zamena matrice matricom koja ima jednostavniju formu;
- Zamena komplikovanih funkcija funkcijama koje imaju jednostavniju formu kao što su to polinomi;
- Zamena nelinearnih problema linearnim problemima čije je rešenje isto ili dovoljno blisko;
- Zamena diferencijalnih jednačina algebarskim;
- Zamena sistema velikog reda sistemima manjeg reda;
- Zamena kontinualnog vremena diskretnim vremenskim koracima.

Ovde treba napomenuti da prilikom svakog koraka moramo paziti da rešenje ostane isto ili približno isto.

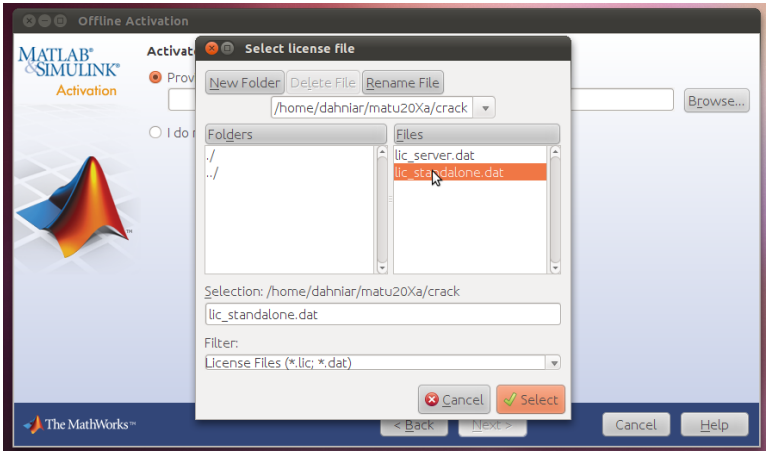
Na primer, sistem nelinearnih diferencijalnih jednačina možemo zameniti sistemom nelinearnih algebarskih jednačina pa taj sistem svesti na linearni sistem algebarskih jednačina za koji imamo metod kako da rešimo.

Softver

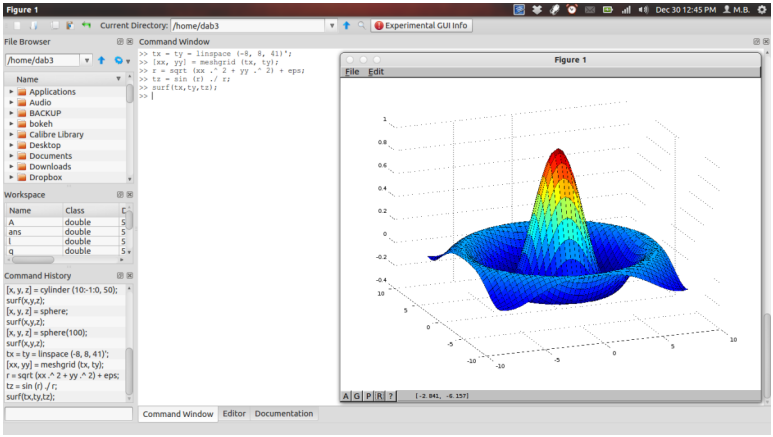
Pre nego što krenemo u dalje razmišljanje o konkretnim problemima, trebalo bi prvo da vidimo šta nam je na raspolaganju od softverskih alata. Ovde želimo da ukažemo na potrebu da se koriste postojeći alati i da nema potrebe praviti svoje osim ako vam nije cilj učenje kako ti alati funkcionišu. Uvek je bolje koristiti nešto što postoji i što je testirano kako bismo mogli da se fokusiramo na ključan problem koji rešavamo i koji je zapravo razlog korišćenja tog alata.

Evo i softvera koji izdvajamo:

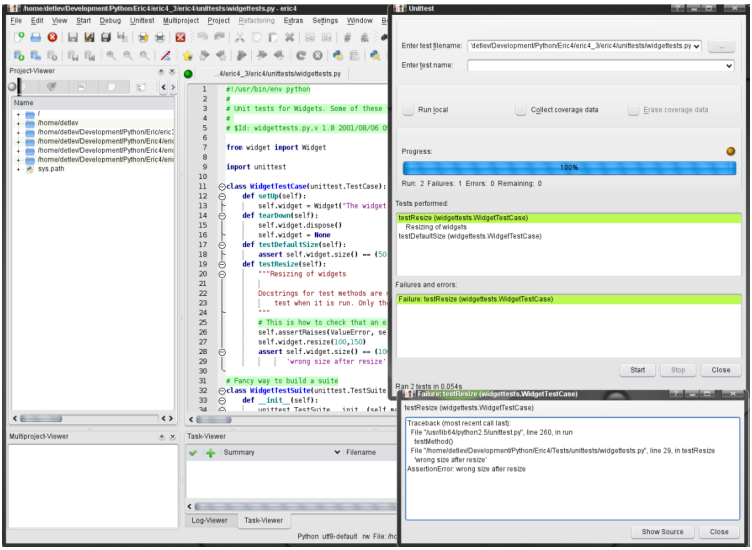
Matlab: komercijalni softver za koji ste verovatno čuli od kolega, ili ste ga koristili u školi. Pošto je ovo časopis o slobodnom softveru, nećemo se previše udubljivati u njegovu funkcionalnost, ali ne možemo reći da ga ne vredi pomenuti, uz napomenu da postoje dobre slobodne alternative koje čak imaju i sličnu sintaksu.



Oktava (eng. *Octave*): slobodna alternativa Matlabu sa kompatibilnom sintaksom.



Pajton (eng. *Python*) sa **Numpajem** (eng. *NumPy*) i srodnim bibliotekama: Uz pomoć malo programiranja možete napraviti značajne rezultate u ovakvom okruženju. Ovo je strogo preporučljivo ako ste do sada radili sa Pajtonom.



Procesing (eng. *Processing*): okruženje namenjeno početnicima u programiranju koje nije bogato koliko gorenavedeni alati, ali pruža mogućnost brzog učenja pa je tako odličan izbor za nekoga ko se prvi put susreće sa programiranjem, a nije mu zanimljivo da počne sa učenjem tako što će praviti konzolne aplikacije.

Za kraj

U narednim brojevima ćemo pokazati primere numeričkih simulacija i obrade podataka u Pajtonu i diskutovati o raznim metodama. Nadamo se da ćemo na ovaj način podstaći deo naših čitalaca da počnu da se zanimaju za ovu oblast, pa i da krenu sa nekim svojim projektima koje će moći da predstave i u našem časopisu.

Ako imate pitanja ili predloge, tu smo da vas saslušamo! Kontaktirajte s nama preko Fejsbuka i Tvitera, ili nam pišite na našu adresu elektronske pošte.

P=NP problem

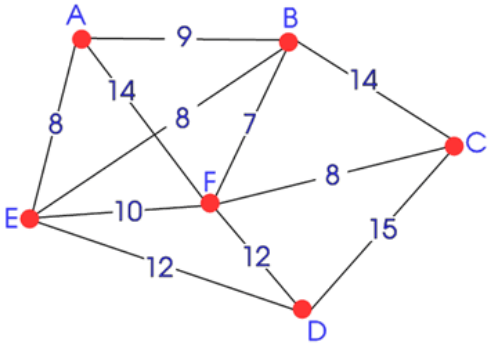
Autor: Luka Hadži-Đokić

Od svog začetka, teorijsko računarstvo bavilo se rešavanjem problema uz pomoć opipljivih ili zamišljenih mašina koje pokreću i izvršavaju algoritme. Ono što su primetili matematičari i računarski naučnici koji su se ovim bavili jeste da postoje problemi koji su nerešivi, dok su kasnije našli da se oni rešivi lako mogu razvrstati po vremenu (ili memoriji) koje je potrebno da bi se algoritam izvršio. Tako je nastala teorija izračunljivosti, a kasnije i ovaj naizgled lak (a posle temeljne inspekcije đavolski težak) problem: „Koji je odnos klasa P i NP?", poznatiji kao „P=NP" problem. Njega su formalno definisali (nezavisno jedan od drugog) Stiven Kuk (eng. *Stephen Cook*) i Leonid Levin, 1971. godine. Uvidevši moguće posledice koje bi izazvalo rešenje, 2000. godine je zajedno sa još šest drugih otvorenih pitanja svrstan među „Milenijumske probleme", pa je tako nagrada za njegovo savladavanje u iznosu od milion dolara ponuđena od strane Klejovog matematičkog instituta (eng. *Clay Mathematics Institute*). Kao uvod u problem, moramo prvo definisati šta tačno znače P i NP.

Klasa P predstavlja one probleme koji se za ulazni podatak veličine n mogu rešiti u c·nk koraka (polinomijalno vreme rešavanja), gde su c i k nepromenljivi (ne zavise od veličine ulaznog podatka). Klasa NP predstavlja probleme čije je rešenje moguće proveriti polinomijalnim algoritmom. Ovo se u neformalnom govoru može objasniti na sledeći način: u klasu P spadaju problemi koji se lako rešavaju, a u klasu NP spadaju oni koji se lako proveravaju. Iz ove definicije izvodimo da svi problemi iz P spadaju i u NP klasu, jer ono što je lako rešiti, lako je i proveriti.

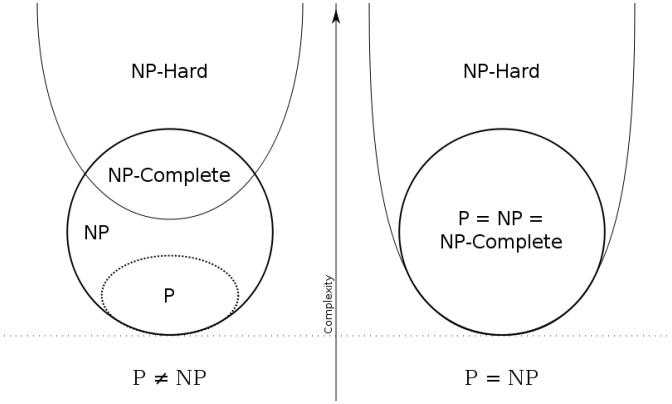
Ostatak NP čine problemi do čijeg se rešenja dolazi teško, u c·kn koraka (eksponencijalno vreme izvršavanja), ali se ipak ono lako potvrđuje. Primer za ovo bi bio problem nalik sledećem: „U nekom studentskom domu treba izabrati

100 studenata od ukupno 400 koji mogu biti primljeni u dom. Uz zadatak, dobili smo i listu parova učenika koji, iz nama nepoznatih razloga, ne smeju biti zajedno na spisku.” Da bismo napravili raspored, jedino što možemo uraditi jeste da probamo sve moguće kombinacije „student-soba” i da potom svaku uporedimo sa listom koju smo dobili. Od 400 studenata izabrati odgovarajućih 100 je praktično nemoguće, jer broj mogućih kombinacija nadmašuje ukupan broj atoma u nama poznatom univerzumu (za neke manje brojeve je moguće rešiti, ali broj koraka naglo raste sa povećanjem ulaznog podatka). U odnosu na to, da bismo proverili jedno rešenje ovog problema, sve što treba da uradimo jeste da izabranih 100 uporedimo sa listom.



Još jedan bitan slučaj klase NP su NP-kompletni problemi – specifični su po tome što se svaki drugi problem iz klase NP na njih može svesti. Tu spadaju problemi trgovačkog putnika, problem zadovoljivosti (SAT problem, koji je u stvari prvi dokazan kao član NP-kompletnih problema, Kuk-Levinovom teoremom) i mnogi drugi. Trgovački putnik je, na primer, problem koji postavlja pitanje da li je, uz pomoć karte sa nekim gradovima i dužine puta između svakog grada, moguće proći kroz svaki od tih gradova i vratiti se u početni, tako da dužina celog puta bude manja od proizvoljno izabrane dužine L. Kada bi neko za ovaj ili neki od ostalih takvih problema našao „lako” rešenje (ono koje se izvršava u polinomijalnom vremenu) i tako ga svrstao u grupu P, dokazao bi da se, u stvari, cela grupa NP može svesti na jedan P problem, što bi dovelo do njihove jednakosti (P=NP). Ovakvo rešenje tog gigantskog pitanja računarstva imalo bi, bez preterivanja, u isto vreme užasavajući i ohrabrujući efekat. Naime, ako bi ono bilo istinito, šifrovanje podataka bi izgubilo svoj smisao (jer se oni šifruju pod pretpostavkom da je jedan problem koji spada u NP skoro nemoguće rešiti), ali bi isto tako i omogućilo lako rešavanje mnogih drugih problema. Kako je to rekao dr Skot Aronson (eng. *Scott Aaronson*) sa MIT-a: „Ako je P=NP, onda bi svet bio dosta drugačije mesto nego što mi pretpostavljamo da jeste. 'Kreativni skokovi' ne bi imali nikakvu specijalnu vrednost, osnovna praznina između rešavanja

problema i prepoznavanja njegovog već pronađenog rešenja takođe bi nestala. Svako ko shvata vrednost simfonije postao bi Mocart; svako ko može da proprati korake argumenta bio bi Gaus."



Međutim, ako je verovati stručnjacima, čije je znanje i shvatanje ovog problema na mnogo višem nivou od nas koji o njemu pročitamo u časopisu ili drugde na internetu, tako nešto je vrlo malo verovatno. U anketi sprovedenoj 2002. godine, od 100 računarskih naučnika 61 je mišljenja da je odgovor P≠NP, njih 22 nije bilo sigurno, 8 je verovalo da je dolaženje do rešenja nemoguće, dok je samo 9 njih reklo da je odgovor P=NP.

Uprkos tome, i uprkos činjenici da već više od četrdeset godina dokaz ne postoji (iako se radi o jednom od najpoznatijih problema u matematici ili računarstvu), mnogi budući ili trenutni umovi naše planete izlazili su u javnost sa „rešenjem" i zbog toga su bili ili ismevani ili prosto ignorisani od strane stručnog kadra. Dok se slažemo da je za rešenje potrebna disciplina i usavršen matematički um (koji se stiče godinama rada u ovom polju), nadamo se da će saznanje o ovom problemu (uz našu pomoć ili pomoć svemogućeg interneta) inspirisati dovoljno genijalnih ljudi da se, počevši od formalnog obrazovanja (praćenog mukotrpnim istraživanjem ove grane računarske nauke), sudare sa P i NP i zaista pobede, a sa današnjim akademicima duboko saosećamo, jer će biti primorani da čitaju sve one očigledno netačne dokaze matematičara u pokušaju dok se ne nađe onaj pravi.

Server

Enkriptovanje i kopiranje servera korišćenjem Duplisiti programa

Autor: Nenad Marjanović

Nekada je većina sistemskih administratora koristila FTP u svrhe čuvanja kopije podataka. Vremenom je utvrđeno da je ovaj način nesiguran i da je svakom ozbiljnom poslovanju zaštita podataka prioritet. Ako smo uspešno zaštitili svoju infrastrukturu, potrebno je zaštititi i čuvanje rezervne kopije podataka. Za to koristimo enkripciju, odnosno šifrovanje podataka.

U ovom procesu opisaćemo instalaciju programa Duplisiti (eng. *Duplicity*) na serverima sa Debijanom i Red Hetom. Za početak, instalirajmo Duplisiti:

```
yum update  &&  yum install epel-release
```

Zatim,

```
yum install duplicity
```

Za Debijan i njegove derivate:

```
aptitude update  &&  aptitude install duplicity
```

Za transfer između dva servera možemo koristiti nekoliko metoda, kao što su R-sink (eng. *rsync*), ranije pomenuti FTP, SCP, SSH, SFTP i druge. U ovom primeru koristimo **SFTP**.

Za potrebe ovog uputstva, CentOS 7 sistem se nalazi na glavnom serveru, a za čuvanje kopija datoteka, server sa Debijanom 8.

Za potrebe transfera i za komunikaciju između ove dve mašine, potrebno je kreirati SSH ključ na CentOS sistemu.

```
ssh-keygen -t rsa -b 2048
```

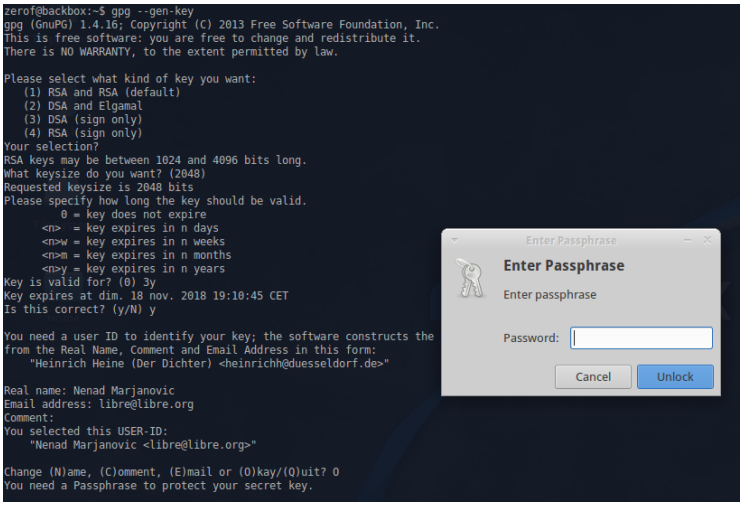
Zatim kopiramo dobijeni ključ na naš udaljeni (eng. *backup*) server, u ovom slučaju uređaj sa Debijanom.

```
ssh-copy-id -p xxxx root@1.2.3.4
```

Vrednosti **xxxx** zamenite portom koji je namenjen SSH komunikaciji, a **1.2.3.4** sa aj-pi (eng. *IP*) adresom servera sa Debijanom 8.

Za potrebe enkriptovanja datoteka kreiramo gpg ključ. Ponuđene opcije tokom ovog procesa su:

- tip ključa koji ćemo koristiti (biramo *RSA*),
- veličina ključa (unosimo 2048, ili samo „Enter”),
- dužina validnosti ključa (ne duže od tri godine — *3y*),
- lozinka (ne kraća od osam karaktera).



Potrebno je u otvorenom terminalu pokrenuti „miš” u svrhu generisanja ključa. Na kraju proverimo da li smo uspešno izvršili prethodnu akciju.

```
gpg -list-keys
```

```
zerof@backbox:~$ gpg --list-keys
/home/zerof/.gnupg/pubring.gpg
------------------------------
pub   2048R/F8DAA8FC 2015-11-19 [expires: 2018-11-18]
uid                  Nenad Marjanovic <libre@libre.org>
sub   2048R/1ECF3CB4 2015-11-19 [expires: 2018-11-18]
```

Javni ključ koji ćemo koristiti za enkripciju datoteke je *F8DAA8FC*.

U daljem procesu povežemo se na server sa Debijanom i kreiramo fasciklu u kojoj ćemo čuvati kopiju podataka. To radimo komandom:

```
mkdir -p /kopija/centos7
```

Ovo je ujedno i jedina komanda koju ćemo pokrenuti u čitavom procesu na serveru sa Debijanom, mada kasnije možemo proveriti veličinu rezervne kopije i slično.

Vreme je da napravimo našu prvu kopiju podataka. U ovom primeru kopiramo **log** datoteke, sa izuzetkom Apačijevih (eng. *Apache*) i Maj-es-kju-elovih (eng. *MySQL*) logova:

```
PASSPHRASE="LozinkaGPGKljuca"  duplicity --encrypt-key javni-kljuc-
ovde --exclude   /var/log/apache --exclude /var/log/mysql /var/log
scp://root@1.2.3.4:xxxx//kopija/centos7
```

Restauracija podataka korišćenjem Duplisitija

Ono što je karakteristično za Duplisiti je da u ovom slučaju na mašini sa CentOS-om moramo ukloniti fasciklu, dokument ili kompresovanu datoteku ukoliko oni već postoje. Ovo radimo u većini slučajeva kada su podaci korumpirani ili izbrisani i kada nam je potrebna njihova rekonstrukcija.

U ovom primeru radićemo sa Endžiniksovim (eng. *nginx*) logovima:

```
rm -f /var/log/nginx
```

Zatim pokrećemo Duplisiti:

```
PASSPHRASE="LozinkaGPGKljuca"  duplicity --file-to-restore
ime_fajla sftp://root@1.2.3.4:xxxx//kopija/centos7 /var/log/nginx
```

Duplisiti ima i druge integrisane funkcije.

Listanje arhiva:

```
duplicity list-current-files
sftp://root@1.2.3.4:xxxx//kopija/centos7
```

Brisanje kopija starijih od nekog perioda (u ovom slučaju šest meseci — **6M**):

```
duplicity remove-older-than 6M
sftp://root@1.2.3.4:xxxx//kopija/centos7
```

Restauracija datoteke stare četiri dana i dva sata:

```
duplicity -t 4D2h --file-to-restore var/log/nekifajl
sftp://root@1.2.3.4:xxxx//kopija/centos7 /var/log/nekifajl
```

U poslednjem primeru koristimo funkciju *-t* koja nam omogućava da preciziramo određene periode kao što su **s**, **m**, **h**, **D**, **W**, **M**, i **Y** (sekundu, minut, sat, dan, nedelju, mesec i godinu).

Na kraju ćemo napomenuti da više detalja o mogućnostima Duplisiti programa možete pronaći na sajtu autora http://duplicity.nongnu.org/index.html.

Mobilni kutak

F-Droid

Autor: Nikola Todorović

Vlasnici pametnih uređaja sa Androidom najčešće instaliraju aplikacije putem Gugl plej prodavnice, neki sa Amazonove prodavnice aplikacija ili nekog nepoznatog izvora. Većina aplikacija koje ste dobili od Guglove ili Amazonove prodavnice su vlasničke[1], a veliki broj njih prikuplja vaše podatke. Jedini izbor koji vam preostaje je, ukoliko želite besplatne aplikacije otvorenog koda, F-Droid.

F-Droid je prodavnica besplatnih aplikacija otvorenog koda za Android platformu. Radi po principu Gugl plej prodavnice. Aplikacije mogu da se pretražuju i instaliraju direktno sa F-Droidovog veb-sajta ili putem Android aplikacije, i sve to bez otvaranja korisničkog naloga.

Karakteristike

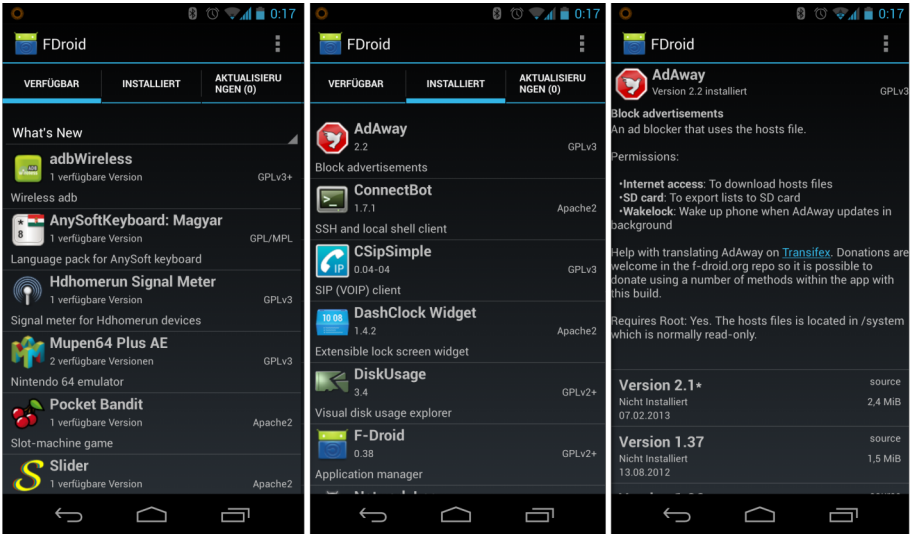
Putem Android aplikacije možete lakše da pretražujete, instalirate i ažurirate aplikacije na vašem uređaju. Pored toga, imate pristup vestima, recenzijama i drugim funkcijama koje pokrivaju sve u vezi sa Androidom i slobodnim softverom. F-Droidova riznica sadrži oko hiljadu petsto pedeset aplikacija i ovaj

[1] vlasničke aplikacije su kompjuterski softver licenciran pod strogim zakonom koji propisuje prava vlasnika. Primaocu ove licence se daje pravo da koristi softver pod određenim uslovima, dok se zabranjuju druge vrste korišćenja poput menjanja, dalje distribucije ili obrnutog inžinjeringa.

broj konstantno raste. Aplikacije su podeljene u dvadeset kategorija — od naučnih, edukativnih i sistemskih, pa do igrica.

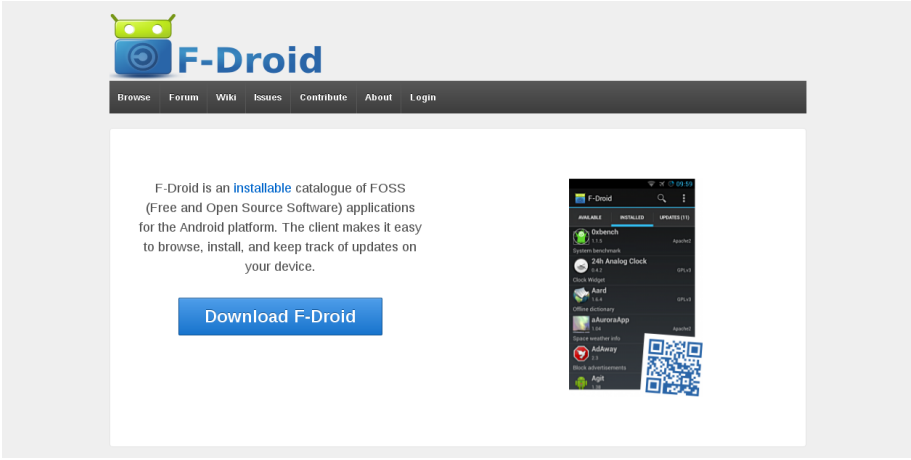
Vaša privatnost se poštuje. Samim tim što ne morate da kreirate korisnički nalog, vi ne odajete vaše podatke, a sama aplikacija ne prati koje ste aplikacije instalirali putem F-Droid prodavnice. Projekat je objavljen pod trećom verzijom Gnuove Opšte javne licence.

Aplikacije mogu biti direktno poslate drugim uređajima preko blututa ili Android bima (NFC + blutut). Mnogo posla je urađeno pa je sada omogućena podrška za Tor i povećana je podrška ažuriranja. Pored mogućnosti preuzimanja aplikacija, omogućen je pristup izvornom kodu aplikacija. Uz recenziju aplikacije nalazi se i upozorenje ukoliko željena aplikacija koristi vaše podatke, sadrži reklame, promoviše vlasnički softver, izvorni kod nije u potpunosti dostupan itd. Postoji mogućnost, za razliku od Gugl plej prodavnice, instaliranja starije verzije određene aplikacije, što je i prikazano na slici ispod.



Instalacija

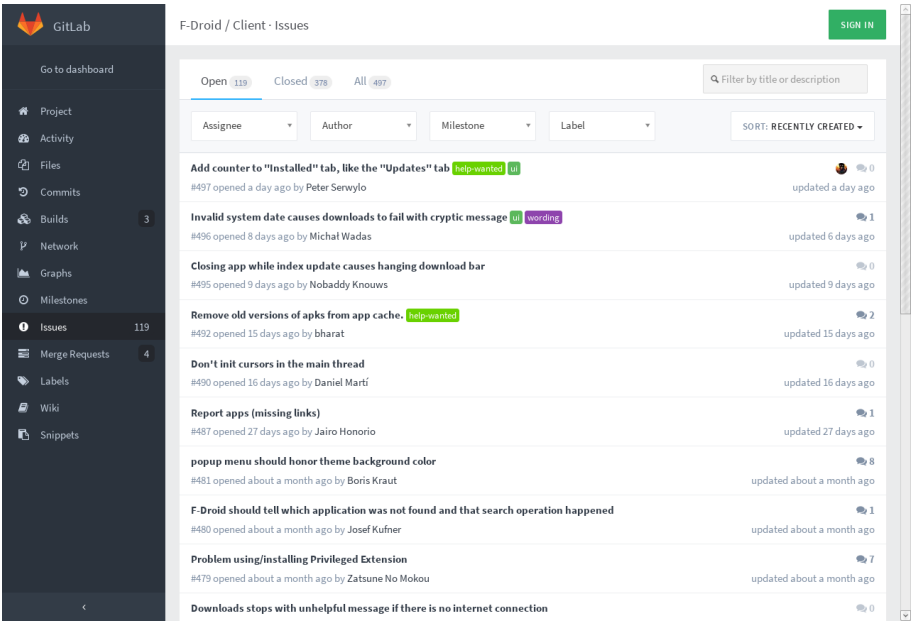
Android aplikaciju možete instalirati sa veb-sajta ili skeniranjem kju-ar koda ispod. U svakom slučaju moraćete da odobrite instalaciju aplikacija sa nepoznatih izvora. Da biste to učinili, uđite u podešavanja. Potom, uđite u bezbednost i tu odobrite instalaciju sa nepoznatog izvora.



Podržite projekat

Projekat u potpunosti razvijaju i održavaju volonteri. Vi takođe možete pomoći na sledeći način:

- Prijavljivanjem problema — ukoliko naiđete na problem sa veb-sajtom ili aplikacijom, možete ga prijaviti na https://f-droid.org/issues/ ili podeliti na forumu i IRC kanalu *#fdroid* na Frinodu (*freenode*);



- Prijavljivanjem aplikacija — ukoliko primetite da neka aplikacija nedostaje u riznici, slobodno to prijavite na forumu;
- Prevođenjem — Android aplikacija je dostupna na mnogo jezika, ali ukoliko vaš jezik nije uključen, ili ako postoji potreba za ispravkom i poboljšanjem prevoda, možete pronaći dalja uputstva kako da pomognete u posebnoj sekciji o prevođenju na forumu;
- Pomaganjem u razvoju — postoje tri Git-riznice koja se čuvaju na Gitlabu. Njima ima pristup svako ko želi da pomogne u razvoju aplikacije i veb-sajta.

Pozivamo vas da 30. januara 2016. godine (subota) u 10 sati učestvujete na akreditovanoj konferenciji koju organiziju Udruženje profesora informatike Srbije, iz Novog Sada uz podršku Centra za promociju nauke iz Beograda.

Konferencija će se održati u prostorijama Karlovačke gimnazije u Sremskim Karlovcima

KONFERENCIJA „SLOBODAN SOFTVER U NASTAVI"

(sa međunarodnim učešćem)

Teme konferencije:

- Primena slobodnog softvera u obrazovanju (osnovne, srednje škole i univerzitet),
- Slobodan softver u inkluzivnom obrazovanju,
- Slobodan softver u XXI veku, tendencije razvoja i novosti,
- Slobodan softver i nauka (primena u raznim naučnim oblastima),
- Slobodne veb-tehnologije,
- Operativni sistemi otvorenog koda,
- Softverske licence (pojam, objašnjenja)
- Slobodan softver u privredi, komercijalnim i finansijskim delatnostima i drugo,
- Hardver i slobodan softver,
- Istraživanja o primeni slobodnog softvera u obrazovanju i nauci,
- Slobodan softver vs besplatan softver,
- Klaud kompjuting u nastavi.

Učesnik može da predloži novu temu koju će razmotriti Programski odbor konferencije. Prijave radova učesnika možete predati do 20.01.2016. godine, do 12 sati.

Više informacija o uslovima prijave možete videti na sajtu konferencije: http://slobodansoftverzaskole.org/konferencija/

Organizacioni odbor konferencije.

Udruženje profesora informatike Srbije
Pasterova 14/11, Novi Sad
Tel. 060/3020748
E mail: upis.ks@gmail.com