

Јул-Август 2015. Број 38

ЛИБРЕ!

Часопис о слободном софтверу



Hack

Play

Learn

Socialize

У сусрет трећем Балканском рачунарском конгресу



ЈОШ ИЗДВАЈАМО

Сигурно брисање података
Команде у ГНУ/Линуксу



Creative Commons Ауторство-Некомерцијално-Делити под истим условима

Реч уредника

Паклено лето 2015. и Балкон

Преживели смо једно од најпакленијих лета до сада. Чак и најстарији чланови редакције се не сећају лета са оволиким бројем тропских дана са температуром изнад тридесет пет степени у хладу. Временске прилике су заиста биле „паралишуће“. У таквим условима нормалан човек мисли само на то како да побегне и расхлади се у некој води (реци, језеру, мору или лавору).

Није тајна да часопис сваке године у летњем периоду има проблема. Годишњи одмори, распуст и висока температура доводе до тога да се редакција „разбежи“ и тада не можемо да функционишемо на уобичајени начин. Можда нам је требало много времена (три године) да схватимо, али научили смо лекцију. Летње време је време за објављивање већ припремљених серијала (специјалних издања часописа), а не за редовне бројеве. Специјална издања захтевају много мање људи од редовних бројева, а и даље одају утисак да часопис функционише и корисни су јер обухватају серијале који су објављивани у више редовних бројева па корисник има на једном месту заокружене најважније теме које је часопис објављивао.

Летњи период не утиче само на редакцију. По статистици преузимања часописа се види да је у том периоду и мање читалаца. Све то указује на неопходност промене политике часописа у овом периоду. Ове године овај двоброј је преседан за часопис. Од следеће године то ће бити уобичајена пракса. У летњем периоду ћемо објављивати један двоброј, а празнину ћемо попунити специјалним бројем.

Срећа за часопис, а такође и за целокупну заједницу слободног софтвера у Србији, што је након овог опуштеног летњег периода организован Балкон (*BalCCon* – Балкански компјутерски конгрес). То је догађај који има исти значај за заједнице слободног софтвера као Егзит (*EXIT*) за рокере или Гуча за фолкере. Можда тога још нисмо свесни, али то је заиста тако. Овај догађај враћа снагу, енергију и веру у слободни софтвер и да оно што сви заједно радимо има смисао на светском нивоу.



Балкон је вршњак ЛиБРЕ! часописа и пролази кроз исте развојне фазе. Прве године је био срећан само зато што је организација успела. Друге године је био срећан што је успео да понови успех. Трећа година је преломна, тек сад могу да се уоче недостаци, да се подвуче црта и исправљају све грешке које се понављају из године у годину. Радни наслов „Трећа срећа” управо одсликава право стање и ако доживи (немамо разлога да у то сумњамо) четврто издање, то неће бити плод среће него промишљених акција који су плод стечених искустава и исправљања свих дотадашњих грешака.

Време је сад да сви прихватимо Балкон као наш Егзит и Гучу. За такав догађај треба се припремати целе године и то не само као организатор (унапредити организацију свако према својим могућностима а у координацији са главним организаторима), већ и као посетилац. Ако већ не можемо помоћи саму организацију догађаја, сви можемо да се припремимо, да платимо улазницу и на тај начин финансијски помогнемо организацију следећег Балкона.

Срећа ће помоћи „Трећој срећи” да протекне у најбољем реду. На нама је да се тамо окупимо и у директним сусретима разменимо мишљења како све унапредити и тако да вратимо мало пољуљану енергију у пројекат слободног софтвера у Србији. Доказали смо да квалитетних појединаца и појединачних пројеката имамо, само треба да унапредимо организацију свега и више радимо тимски. Досадашње искуство показује да појединачни наступи нису довољни за постизање било каквог циља. За боље резултате потребан нам је тимски дух.

Развијајмо тимски дух и у области која није плодно тле за исти. Програмери су познати као јаки индивидуалци. Са друге стране, слободан софтвер захтева тимски рад. Конгреси попут Балкона су идеална места да се индивидуалци удруже и да развију тимски дух у интересу свих. Видимо се на Балкону, после нам можете писати ваше утиске са њега на нашу већ познату адресу [libre \[et\] lugons \[dot\] org](mailto:libre@lugons.org).

До следећег броја,

ЛиБРЕ! тим

Садржај

Вести

стр. 6

Пул слободе

У сусрет трећем Балканском рачунарском конгресу

стр. 9

Представљамо

Додаци за Опенофис и Либреофис који живот значе

стр. 14

Како да...?

Како проследити Икс преко сигурне шкољке
Сигурно брисање података (1. део)

стр. 20
стр. 24

Ослобађање

Команде у ГНУ/Линуксу (1. део)

стр. 30

Слободни професионалац

Ваш посао, опен-сорс посао (5. део)
Мозила — Од заједнице до корпорације

стр. 34

Интернет мреже и комуникације

Шифровани чет (5. део) - Токс
Облаци и катанци: Сигурни у облацима (1. део)

стр. 39
стр. 45

Моћ слободног
софтвера





ЛИБРЕ! пријатељи



Број: 38

Периодика излажења: месечник

Извршни уредник: Стефан Ножинић

Главни лектор:

Адмир Халилкановић

Лектура:

Јелена Мунђан Сашка Спишјак

Милена Беран Милана Војновић

Александар Божиновић

Александра Ристовић

Графичка обрада:

Дејан Маглов Иван Радељић

Дизајн: White Circle Creative Team

Аутори у овом броју:

Данијел Гомола Петар Симовић

Александар Божиновић Дејан Маглов

Јелена Георгијевић Кресојевић

Остали сарадници у овом броју:

Марко Новаковић Михајло Богдановић

Почасни чланови редакције:

Жељко Попивода Жељко Шарић

Владимир Попадић

Александар Станисављевић

Контакт:

IRC: #floss-magazin на irc.freenode.net

Е-пошта: libre@lugons.org

Вести

23. јун 2015.

Адоби развија слободан кориснички интерфејс за дизајн апликација

Адоби је најавио да развија интерфејс који се базира на ХТМЛ5 за дизајн апликација и веб сајтова, под слободном лиценцом.

Користан линк: <http://j.mp/1ELONwE>



24. јун 2015.

Кјут ће користити модерне Ц++11 могућности

Од верзије 5.7, Кјут (Qt) ће користити више могућности из Ц++11.

Користан линк: <http://t.co/tQKvO8taoU>



24. јун 2015.

Сарадња Ред Хета и Самсунга

Ове две компаније су се удружиле на пољу мобилних технологија.

Користан линк: <http://t.co/7mXqNxUR6g>





25. јун 2015.

Еклипс развојно окружење добија подршку за Докер

Ово окружење добија подршку за Докер од верзије 4.5.



Користан линк: <http://t.co/JcrkZF0qwQ>

9. јул 2015.

Факултет техничких наука у Новом Саду ће на свом РТ-РК одсеку прећи на слободан хардвер

Одсек за рачунарску технику и рачунарску комуникацију ФТН-а прелази на употребу Разбери-Паја и Ардуина на својим лабораторијским вежбама.



Користан линк: <http://j.mp/1PXSWfl>

20. јул 2015.

Вижуал Студио ће имати подршку за Линукс

Мајкрософт је најавио да Вижуал Студио од нове верзије има подршку и за Линукс.



Користан линк: <http://t.co/zrDYYHdz7L>

Вести

20. јул 2015.

Објављен ГЦЦ 5.2

Објављена је нова верзија овог популарног слободног преводиоца.

Користан линк: <http://t.co/xw283Ll8zD>



24. јул 2015.

Ц-мејк 3.3 објављен

Објављена је нова верзија Ц-мејка (CMake), система за превођење и дистрибуцију слободних софтверских решења.

Користан линк: <http://t.co/frgOs21hZZ>



4. август 2015.

Бро, софтвер за заштиту који се налази на већини система влада и компанија, пуни двадесет година

Пре тачно двадесет година Верн Пексон је током својих докторских студија написао софтвер који ће постати један од незаобилазних алата на системима америчке владе.

Користан линк: <http://j.mp/1M6EAej>





У сусрет трећем Балканском рачунарском конгресу

Аутор: Јелена Георгијевић Красојевић



Пул слободе

У Новом Саду ће се, од 11. до 13. септембра у **Музеју савремене уметности Војводине**, одржати трећи по реду регионални хакерски конгрес под слоганом „Балкон 2015 - Трећа срећа“ (*BalCCon2k15 - Third time's a charm*). Први је имао назив **Први контакт**, други је био наставак па смо га назвали **Другом базом**, а надамо се да трећи бити управо **трећа срећа**.

Програм конгреса обухвата бројне презентације, радионице као и предавања из области безбедности рачунарских система, са посебним освртом на друштвено-политичке теме, попут заштите приватности на интернету, слободног софтвера, програмских језика, развоја апликација и бројних других. Предавачи су познати и признати припадници хакерских заједница из целог света.

Организатори конгреса су новосадско удружење корисника Линукса, „ЛУГОНС“, и Фондација Вау Холанд (*Wau Holland*) из Хамбурга. Основни циљ удружења су рад на бољитку друштва и подстицање коришћења ГНУ/Линукс система, како у предузећима, тако и код појединаца и ентузијаста. ЛУГОНС је подршка свим корисницима Линукса, како у Новом Саду и Војводини, тако и у целој Србији. Чланови удружења настоје такође да подигну свест о информатичкој култури и промовишу бесплатан и слободан отворени софтвер.



„Балкон“¹ је замишљен тако да постане центар хакерске заједнице у региону, за све оне који финансијски нису у могућности да посећују друге конгресе у Европи и САД-у. Оваква манифестација неопходна је на Балкану, како би се обезбедило место на коме се једном годишње размењују новостечена знања, састају млади пуни идеја и старији пуни искуства и знања; да се упознају, повежу и охрабре сви које рачунари, мреже, сигурност и неконвенционалан начин размишљања занимају, а немају где да добију жељене информације. Тиме би се у самој

¹ „Балкон“ (BalCCon) - Балкански рачунарски конгрес



хакерској заједници подизао ниво стручности уз вођство старијих колега, а и решио би се проблем немогућности да се допре до простора и времена да се сопствени радови презентују. Довођење познатих и признатих људи да одрже предавања омогућава људима из региона да их виде уживо и да дискутују са њима о темама које их занимају. Балкон жели да приближи свет студентима који се интересују за хактивизам, слободни код и техничке науке, али и свим младима којима су ове и сродне теме интересантне. На овај начин, млади имају прилику да представе своје радове уколико су занимљиви, иновативни и у складу са моралним начелима за које се залаже цела заједница окупљена око слободног кода.

Погледајмо сада ко су предавачи. Хакери, то јесу. Хакер је онај ко своје знање о рачунарима жели да пренесе и подели са другима.

Дођите, јер у супротном пропуштате прилику да чујете, упознате и дружите се са следећим предавачима:

Воја Антонић:

Да ли се неко сећа часописа „Рачунари у вашој кући“, па још првог броја, све са описом самоградње рачунара Галаксија? Упознајте лично њеног творца. Решен је да подели са вама своје знање о електроници, лемљењу и да заједно са њим направите своју конзолу за играње.



Бернд Фикс (Bernd Fix):

Хакер из Берлина који је 1986. године приступио у Хаос компјутер клуб (*Chaos Computer Club*). Творац првог демо вируса који је објављен у часопису Датеншлојдер (*Datenschleuder*). Држи се максиме правог хакера: Не петљај се у туђе податке!². Овај пут на Балкону (*BalCCon*) ће држати радионицу за



² Don't mess around with other people's data.

Пул слободе

новинаре - *Situation Awareness for Journalists*, где ће сви заинтересовани новинари имати прилику да се упознају са новим начином прикупљања информација и њиховим управљањем, те заштитом дигиталног идентитета. Такође, биће предочена важност технологија у данашњем раду.

Травис Гудспид (Travis Goodspeed):

Зар га је потребно додатно представљати? Промотер Балкона по целом свету, и после првог Балкона, опет га можемо видети у Новом Саду, овога пут са темом **Полиглоте у радио-аматеризму** (*Polyglots in Amateur Radio*), где ће говорити о радио сигнаlima и модулацији.



Алук (Aluc):

Организатор Бисајдса (*Bsides*) у Берлину, код нас ће одржати предавање под следећим називом: **Не лажите ме** (*don't lie to me*). Звучи интересантно, надамо се да вас је заинтересовао.

Вирус (Vyrus):

Специјалан гост из САД-а, дођите да чујете његово предавање (*Go)ne Phishing*, о заштити од пецања као напада на рачунарски систем уз помоћ преваре корисника.

Мари Гитбуб (Marie Gutbub):

Рођена у Француској, студирала новинарство у култури на Берлинском Универзитету уметности. Од 2014. године Мари организује Криптопарти (*CryptoParty*) у Берлину и широм Европе, ширећи свест о приватности кроз разговоре и радионице. Она такође држи предавања о безбедносним информацијама за новинаре на неколико универзитета. Као





слободни новинар, она пише, између осталог, и за Фрајтаг³. Код нас ће држати више радионица и предавања: **Криптопарти мора умрети, Долазим у миру** (*CryptoParty must die, I come in peace*) и многа друга.

Петер Бубештингер (Peter Bubestinger):

Координатор од 2008. године у Фондацији слободног софтвера Аустрије, као и вођа пројекта и програмер у области дигитализације аудио-визуелне архиве од 2002. године. Стекао је практично искуство у раду са архивима великих институција као што су аустријска Медијатека (*Mediathek*), РТВ Словеније, СРТЦ (Судан), Глас Вијетнама, Колос (Брисел), ОРФ, фонотека Национал (Мексико) и друге. Тренутно је главни програмер ДВА-Профешна (*DVA - Profession*) – решења за видео дигитализацију архиве, коришћењем слободног софтвера и слободног кода. Од 2008. године је члан екипе „Фондације слободног софтвера Европе“ (*FSFE*) и тренутно координира њихове активности у Аустрији, а држаће предавање чији је назив **ФФmpegов видео кодек без губитака ФФV1** (*FFmpeg's FFV1 lossless video codec*).



Биће присутни и многи други који су подједнако интересантни као претходно наведени предавачи.

Шта још рећи осим – дођите, чујте, видите и пробајте!

Листа предавача није коначна, али је можете пратити на: <https://2k15.balccon.org/speakers/speakers.html>

Уколико смо вас заинтересовали да присуствујете конгресу, резервишите и купите карту на сајту <https://tickets.balccon.org> Такође, уколико имате питања, можете нам се јавити на адресу електронске поште *orga at balccon.org*.

Више о програму и организацији на: <https://balccon.org>.

Званични налог на Твитеру: [@BalCC0n](https://twitter.com/BalCC0n)

³ Der Freitag - Фрајтаг, немачки недељник.

Представљамо

Додаци за Опенофис и Либреофис који живот значе



Аутор: Дејан Маглов

Не можемо замислити ниједан иоле озбиљан текстуални процесор без додатка за аутоматску проверу исправности писања на енглеском језику (енг. *spellcheck*). Енглези нису имали свог Вука Стефановића Караџића и не пишу онако како говоре. Чак и боље образовани Енглези нису увек сигурни како се понека реч исправно спелује и зато им је неопходан додаток за проверу исправности писања. Они би одбацили сваки текстуални процесор који га не би имао.

Са друге стране, ми смо склони да се задовољимо било каквим текстуалним процесором. Не само што нам не недостаје додаток за проверу исправности писања, већ врло често заборављамо да искључимо енглеску проверу писања и аутокоректуру. Зато нам се дешава да у препискама имамо аутоматски исправљено слово „и” тако да је свако исписано великим словом. Штавише, не користимо ни нашу ћирилицу а често ни наша латинична слова, него пишемо „ошишаном” латиницом. У неформалној преписци то можда и није неки проблем, али у формалној преписци то је неписмено.

Да ли чињеница да пишемо како говоримо значи да нам није потребна провера исправности писања? Наше је мишљење да нам је итекако потребна. Људи смо и грешимо у свему па и приликом куцања. „Гутамо” слова, пермутујемо слова, недовољно познајемо нашу граматику, а и питање је колико исправно говоримо.



Ни најбољи додаток за проверу исправности писања нас неће заштитити од свих могућих грешака, али их може смањити и учинити нас мало „писменијим“ него што јесмо, што може да нам значи приликом формалне преписке (писање молби, жалби, захтева и апликација).

Осим провере исправности писања, Срби имају још један проблем који се може решити добрим додатком за текстуални процесор. Енглези пишу само једним писмом, латиницом, а ми се служимо латиницом и ћирилицом. Нама је неопходан и додаток за брзо пресловљавање текста из једног у друго писмо.

По уставу Србије званично писмо у Србији је ћирилица па је обавезно званичну преписку са државним органима вршити на ћирилици. Мука је ако већ имамо барем пола текста припремљено на латиници. Прекуцавање на ћирилицу је тешко, те је један лаки пресловљавач неопходан сваком текстуалном процесору.

ООоТранслит и Правопис и хифенација за српски језик (ћирилица и латиница)

Проблем решавања ових проблема на текстуалним процесорима постоји одавно. Први је комплетно решење понудио пројекат РАС и његов креатор Р. Симић. РАС је решио проблеме провере писања, прелома речи на крају реда, пресловљавање и то за Мајкрософт Офис. Највећи проблем са РАС-ом је био у томе што је то власнички комерцијални софтвер и због тога није био у масовној употреби. Иако

Представљамо

није био скуп, ипак је био везан само за једну машину и само један оперативни систем. Свака реинсталација система би поништила лиценцу што је онда повлачило или нову куповину РАС-а или контактирање са власником како би се добио нови серијски број. То је све било сувише компликовано и због тога пројекат није масовно заживео.

Не знамо колико је РАС донео финансијске користи свом власнику, али знамо да је донео прилично невоља кориснику. Због РАС-а и сличних комерцијалних програма корисници су избегавали да реинсталирају своје оперативне системе да не би поново морали да плаћају те програме. Зато су „крпили“ и „лечили“ већ прилично „бушне“ и вирусима заражене оперативне системе.

Један овакав алат зато мора да буде слободан софтвер, а то подразумева и слободан текстуални процесор. Ово није само питање софтвера него опште културе целокупне нације.



Први слободни додатак „ООоТранслит“ за Опенофисовог Писца и табеларни прорачун (Калк) развио је Александар Урошевић из Крагујевца у мају 2008. године. Својим додатком је решио брзо пресловљавање означеног или целокупног текста документа из ћирилице у латиницу и обрнуто. Овај додатак је постао званични додатак за Опенофис (касније, Либреофис) и може да се преузме са [сајта пројекта](#) или са [страница додатака за Либреофис](#).

Други слободни додатак Опенофисовог Писца „Српски правопис и хифенација (ћирилица и латиница)” (*Serbian (Cyrillic and Latin) Spelling and Hyphenation*) развио је Горан Ракић у децембру 2008. године. Овај додатак увршћен је у званичне додатке за Опенофис (Либреофис) и решио је проблем провере писања и прелома речи на крају реда. Може се преузети са [страница додатака за Либреофис](#).

Инсталација додатака за Либреофис

Верујемо да врло мало људи не зна како се инсталирају додаци у Либреофис, али ћемо ипак укратко појаснити процес за оне који то не знају.



Довољно је само преузети датотеке са екстензијом **OXT** и отворити их Либреофисом (*Open with...* - Отвори помоћу...). Све остало је по принципу Даље/Даље/Даље/Крај (енг. **Next/Next/Next/Finish**). Поновним покретањем Либреофиса додаток ће постати активан, а остало је да евентуално промените подешавања у самом Писцу, на пример да поставите српску ћирилицу (или латиницу) као подразумевани језик за проверу писања и уживате у благодетима које провера исправности писања доноси.

The screenshot shows the OpenOffice.org Extensions website. The main heading is "Serbian (Cyrillic and Latin) Spelling and Hyphenation". The page includes a search bar, navigation links (Home, Search, Templates, Get Apache OpenOffice, Extensions Wiki, Login), and a sidebar with search filters (Search extensions, Dictionaries, Highest Rated, Most Popular, Most Recent). The extension details include:

- Prepared by:** OpenOffice, ЛибреОфис и LibreOffice
- Manufacturer:** gromit99
- Rating:** 4.5 stars (average 2.7 (3 votes))
- Application:** OpenOffice.org
- Tags:** Dictionary
- Screenshots:** <http://extensions.libreoffice.org/>
- Source code:** <http://git.libreoffice.org/dictionaries/>
- Post date:** Tuesday, 19 November 2008 - 25:45
- Statistics:** View: 36 - Month: 120 - Year: 4,822 - Details

Below the details, there is a "Download extension" button and a description in Serbian: "Провера писања и промена речи за српски језик (лат, ћири)". The page also contains a list of authors and a note about the source code being available on GitHub.

Правопис и хифенација за српски језик (ћирилица и латиница)

Овај додаток ради тако што упоређује сваку откуцану реч са својим уграђеним речником. Речник садржи велики број речи са свим подваријантама (различити род, број, падеж и глаголски облик). Уколико додаток пронађе откуцану реч у



нису „њ” и „д ž” нису „џ”. Већину тих изузетака је аутор ООоТранслита идентификовао и аутоматски примењује, али је и даље остало неколико неидентификованих изузетака на које корисници треба да обрате пажњу и провере текст након пресловљавања из латинице у ћирилицу, а у томе им може помоћи претходни додатак (Правопис и хифенација за српски језик).

За крај

И поред несавршености ових алата, они су веома корисни. Смањују број грешака и олакшавају живот приликом примене оба српска писма. Ови додаци су слободни, отвореног кода, бесплатни и за слободне текстуалне процесоре (Опенофис и Либреофис) који раде на свим оперативним системима. Ако и постоји оправдање за коришћење комерцијалних и власничких оперативних система јер не постоје алтернативе за неке видове примене рачунара, за коришћење власничких канцеларијских пакета скоро да нема оправдања. Са овим додацима специфичним за српски језик слободни канцеларијски пакети програма су много кориснији од налицканих власничких без оваквих додатака.

На крају бисмо још поменули проблеме домаће заједнице слободног софтвера. Чини нам се да се можемо сложити да су овакви пројекти од националне важности, а, нажалост, они никад нису били подржани на прави начин ни од државних органа, неке државне институције која се бави информатиком и културом, а ни од саме заједнице слободног софтвера. Пројекти можда јесу мали, али су значајни и могли би да се додатно унапреде. До тога, нажалост, неће доћи јер, осим ентузијазма појединаца који су пројекте подигли на ноге, нема нове мотивације да се они и унапређују.

Наглашавамо и проблеме у које је упао пројекат ООоТранслит пре око годину дана када је претило да потпуно буде угашен и избрисан иако још увек функционише. Једно је развити алат за сопствене потребе и великодушно га поклонити на коришћење свима као слободан софтвер, а друго је додатно плаћати и одржавати га о сопственом трошку без додатне мотивације. То се управо догодило ООоТранслиту и умало није потпуно угашен пројекат и његов сајт. Да није било ЛУГОНС заједнице да га преузме, данас не бисмо писали о овом додатку.

Овај текст посвећујемо свим малим пројектима без којих они већи не би били могући.

Како да...?

Како проследити Икс преко сигурне шкољке?

Аутор: Александар Божиновић

Основни појмови

У информатичким текстовима, неретко оним који се тичу отвореног софтвера, користе се акроними – скраћенице које настају сажимањем више речи у једну. Временом и понављањем акронима нестала је потреба (немарност аутора, прим.аут.) да се, макар у фусноти, наведе његово значење. **Шкољка** (енг. Shell) је назив за програм, односно интерфејс за приступ услугама рачунарског система, попут покретања програма, кретања кроз систем датотека и употребе услуга оперативног система¹. Шкољка као спољашњи омотач мекушаца описује једну додирну површину између корисника и сржи оперативног система. Шкољка нам је позната под називом **терминал**. Два рачунара преко сигурне шкољке остварују сигурну везу која се означава термином **тунел**. **Икс** је део сленга и означава графички приказ свега на екрану. Пун назив је систем прозора Икс (лат. X и X11) и то је протокол за приказ система прозора на екранима који се базирају на пикселима². **ВНЦ** (енг. *Virtual Network Computing*) је софтвер који преноси графички приказ удаљеног рачунара, који се означава као сервер, локалном рачунару, који се означава као клијент. Истовремено команде тастатуре и миша са локалног рачунара преноси удаљеном рачунару. Укратко, ВНЦ се користи за контролисање удаљеног рачунара.³

¹ [https://sr.wikipedia.org/wiki/Љуска_\(рачунарство\)](https://sr.wikipedia.org/wiki/Љуска_(рачунарство))

² https://sr.wikipedia.org/wiki/X_Window_System

³ https://de.wikipedia.org/wiki/Virtual_Network_Computing



Припрема

Замислите следећу ситуацију - желите да контролишете удаљени рачунар, али не желите да користите власничке програме какав је Тимвјувер (енг. *TeamViewer*). Већина власничких програма шаље ај-пи адресу (енг. *IP*) на сервер и све се обавља преко њега. Овај текст укратко описује релативно једноставан начин да се оствари приказ исписа екрана са удаљеног рачунара на локални рачунар у стварном времену, као и како да се кориснику на локалном рачунару омогући контрола удаљеног рачунара. За сврху овог текста коришћена су два рачунара на којима је инсталиран Убунту. Најпре је потребно инсталирати пакете *openssh-server* и *x11vnc* на удаљеном рачунару:

```
sudo apt-get install openssh-server x11vnc
```

На локални рачунар неопходно је инсталирати ВНЦ прегледач, на пример *gtkvncviewer*:

```
sudo apt-get install gtkvncviewer
```

Како да...?

Повезивање

Да бисте проследили Икс, потребно је да укуцате следеће (такође на удаљеном рачунару):

```
x11vnc -rfbport 5900
```

Затим је потребно у ВНЦ прегледник на локалном рачунару унети следеће податке:

```
server: ip_adresa_udaljenog_racunara:5900  
username: korisnicko_ime_udaljenog_racunara  
password: lozinka_udaljenog_racunara
```

Тако ћете отворити прозор с приказом исписа удаљеног рачунара у коме можете користити миш да бисте контролисали удаљени рачунар. Имајте на уму да прекидом везе ви проузрокујете прекид рада програма *x11vnc* на удаљеном рачунару. Да би он остао активан и по прекиду везе, потребно га је покренути с додатком аргумента *forever*.

```
x11vnc -rfbport 5900 --forever
```

Прослеђивање порта

Када се удаљени рачунар налази у мрежи коју регулише рутер, портови су сигурно „затворени“. То се може решити остваривањем тзв. реверзног тунела или везе (енг. *SSH reverse tunneling*). То заправо значи да удаљена машина обезбеђује локалној машини приступ свом порту. Нека порт А буде порт локалне машине, а порт Б порт удаљене машине. Када се реверзни тунел успостави, преко порта А на локалној машини приступа се порту Б на удаљеној машини. Притом се подразумева да су порт локалне машине и рутер „испред“ локалне машине „отворени“ (порт 22). Порт 22 је иначе подразумевани порт за сигурну шкољку.

Реверзни тунел остварује се са удаљеног рачунара.

```
ssh -R 12345:localhost:5900  
korisnicko_ime_udaljenog_racunara@ip_adresa_udaljenog_racunara
```



Икс преко сигурне шкољке

У овом примеру, 12345 је порт локалне машине (А), а 5900 је порт удаљене машине (Б).

Након тога, потребно је покренути `x11vnc` (такође на удаљеном рачунару):

```
x11vnc -rfbport 5900
```

Покрените ВНЦ прегледник на локалном рачунару и унесите следеће податке:

```
server: localhost:12345  
username: korisničko_ime_udaljenog_računara  
password: lozinka_udaljenog_računara
```

```
Terminal  
File Edit View Terminal Tabs Help  
aleksa@N61PB-M25:~$ ssh -R 12345;localhost:5900 stefan@212.178.250.39  
The authenticity of host '212.178.250.39 (212.178.250.39)' can't be established.  
ECDSA key fingerprint is de:29:f4:43:c1:a6:93:d6:ac:3d:97:8a:b8:f4:41:a6.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '212.178.250.39' (ECDSA) to the list of known hosts.  
stefan@212.178.250.39's password: █
```

Како да...?

Сигурно брисање података (1. део)

Аутор: Petar SImović

Иако можда на својим рачунарима немамо државне тајне или забрањени садржај који нам лако могу обезбедити карту за боравак иза решетака, ипак, не шкоди знати како се фајлови на рачунарима свакодневно (не) бришу и како их можемо стварно неповратно обрисати. Подаци на рачунарима могу бити смештени у различите врсте меморија, па је начин њиховог брисања, као и самог записивања директно условљен самим физичким особинама медијума. Овде ћемо се позабавити сигурним брисањем података са хард дискова и новијих полупроводничких дискова (ССД), као и са УСБ меморија, флеш картица, оперативних меморија (RAM), и тзв. своп (енг. *swap*) партиција на дисковима.

Увод

Брисање фајлова заправо не постоји, постоји само преписивање новог садржаја на место старог. Да бисмо ово разумели, морамо знати како оперативни систем води рачуна о томе шта на диску јесте податак, а шта није. Оперативни систем води своју табелу или дневник шта је где уписано и која меморија је на диску слободна, тако да када уписујемо неки податак, оперативни систем проверава своју табелу и види где има места да се податак упише; проследи га диску, и тај простор означи у својој табели као заузет. Затим се запише и показивач (адреса) на тај податак на диску. Међутим, сада долази занимљив део. Када фајл треба обрисати, оперативни систем само обрише показивач у својој табели, и то место означи као слободно, а подаци на диску остају нетакнути док се преко њих не упише неки нови податак. Знајући ово, једино решење за сигурно брисање података представља преписивање нових података преко старих, како се стари не би могли повратити.



Хард диск

За сигурно брисање података на ГНУ/Линукс системима можемо се послужити програмом **Шред** (енг. *Shred*) који је подразумевано укључен у све ГНУ-ове дистрибуције. Треба прво напоменути да овај програм неће обрисати податак у смислу да неће бити видљиво да је фајл ту био, већ ће фајл преписати новим садржајем, остављајући оригинално име фајла у директоријуму, као и нечитљиви и неповратни оригинал преписан новим насумичним садржајем. Да бисте ово испробали, направите копију неког фајла и онда га обришите опцијом:

```
shred -v FILE_NAME
```

```
Terminal
petar@travelmate: ~/Laboratory/Delete 3 is
usage: shred [OPTION]... FILE...
Overwrite the specified FILE(s) repeatedly, in order to make it harder
for even very expensive hardware probing to recover the data.

Mandatory arguments to long options are mandatory for short options too.
  -f, --force          change permissions to allow writing if necessary
  -n, --iteration=N   overwrite N times instead of the default (3)
  --random-source=FILE get random bytes from FILE
  -s, --size=N        shred this many bytes (suffixes like K, M, G accepted)
  -u, --remove        truncate and remove file after overwriting
  -v, --verbose       show progress
  -x, --exact         do not round file sizes up to the next full block;
                    this is the default for non-regular files
  -z, --zero          add a final overwrite with zeros to hide shredding
  -h, --help          display this help and exit
  --version          output version information and exit

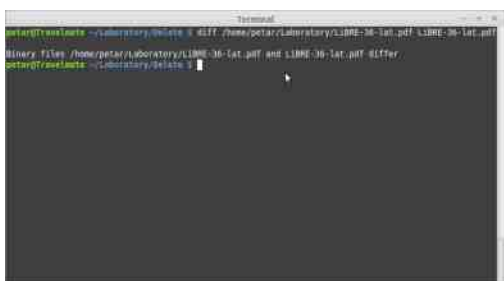
If FILE is -, shred standard output.

Delete FILE(s) if --remove (-u) is specified. The default is not to remove
the files because it is common to operate on device files like /dev/ada,
and those files usually should not be removed. When operating on regular
files, most people use the --remove option.
```

```
Terminal
petar@travelmate: ~/Laboratory/Delete 3 is
LIBRE-35-lat.pdf LIBRE-36-lat.pdf LIBRE-37-lat.pdf
petar@travelmate: ~/Laboratory/Delete 3 shred -v LIBRE-36-lat.pdf
shred: LIBRE-36-lat.pdf: pass 1/3 (random)...
shred: LIBRE-36-lat.pdf: pass 2/3 (random)...
shred: LIBRE-36-lat.pdf: pass 3/3 (random)...
petar@travelmate: ~/Laboratory/Delete 3
```

После овога можете приметити да је фајл и даље остао у директоријуму, али га не можете отворити, а ако га програмом *Диф* (енг. *diff*) упоредите са оригиналом, видећете да се фајлови разликују, као што можете приметити ако их погледате под лупом неким хекс (енг. *hex*) едитором. Наравно, фајл може бити обрисан колико год пута желите опцијом *n* после које морате унети број пута пребрисавања фајла, а подразумеван број пребрисавања фајла је три, уколико није назначено другачије. Постоји и опција *z* која додаје још једно пребрисавање нулама на крају, како би се прикрило да је фајл уопште постојао и био брисан, мада ово више има смисла ако после уклоните фајл из директоријума и из кантице за смеће.

Како да...?



```
shred -vn 10 FILE_NAME
```

Тачан број пута колико је потребно да неки фајл пребришете новим садржајем није назначен. Тачније овај магичан број се одређује и на основу типа медијума са кога се фајл жели обрисати. На пример, Гутманова метода за сигурно брисање <https://goo.gl/oyCpBn> (енг. Gutmann method for secure deletion) пребрисује фајлове тридесет и пет пута, док **срм** (енг. *srm*) програм то ради тридесет и осам пута подразумевано. Треба напоменути да је ово важило за дискове из деведесетих година прошлог века, док се за данашње дискове, изузев флеш меморија (ССД,



Сигурно брисање података

УСБ и СД картице), препоручује три до седам пута (<https://goo.gl/084snA>).

Уколико желимо да обришемо фајл тако да се ни не примети да је ту пре био, можемо користити **срм** програм кога претходно морамо инсталирати.

```
sudo apt-get install secure-delete
```

Након тога покрећемо овај програм из терминала командом *srm* и бришемо неки фајл.

```
srm -v FILE_NAME
```

```
Terminal
netar@7:~$ls -la ~/Library/Delete.1 ls
LIBRE-35-lat.pdf LIBRE-36-lat.pdf LIBRE-37-lat.pdf
netar@7:~$ls -la ~/Library/Delete.1 srm --help
srm v3.1 (c) 1997-2003 by van Hauser / TMC <vha@tmc.org>
Syntax: srm [-dflrvz] file|filez etc.
Options:
-d ignore the two dot special files "." and "..".
-f fast (and insecure mode): no /dev/urandom, no synchronize mode.
-l lessens the security (use twice for total insecure mode).
-r recursive mode, deletes all subdirectories.
-s is verbose mode.
-z last wipe writes zeros instead of random data.
srm does a secure overwrite/removes/delete of the target file(s).
Default is secure mode (3R writes).
You can find updates at http://www.tmc.org
netar@7:~$ls -la ~/Library/Delete.1
```

```
Terminal
netar@7:~$ls -la ~/Library/Delete.1 ls
LIBRE-35-lat.pdf LIBRE-36-lat.pdf LIBRE-37-lat.pdf
netar@7:~$ls -la ~/Library/Delete.1 srm --help
srm v3.1 (c) 1997-2003 by van Hauser / TMC <vha@tmc.org>
Syntax: srm [-dflrvz] file|filez etc.
Options:
-d ignore the two dot special files "." and "..".
-f fast (and insecure mode): no /dev/urandom, no synchronize mode.
-l lessens the security (use twice for total insecure mode).
-r recursive mode, deletes all subdirectories.
-s is verbose mode.
-z last wipe writes zeros instead of random data.
srm does a secure overwrite/removes/delete of the target file(s).
Default is secure mode (3R writes).
You can find updates at http://www.tmc.org
netar@7:~$ls -la ~/Library/Delete.1 srm -rz LIBRE-36-lat.pdf
Using /dev/urandom for random input.
Wipe mode is secure (3R special passes)
*****
netar@7:~$ls -la ~/Library/Delete.1
```

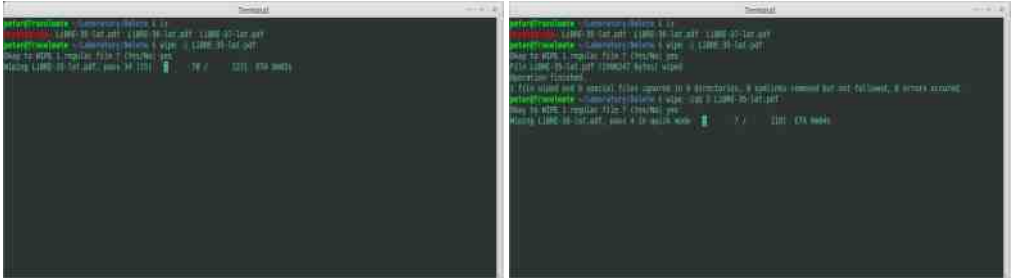
Тиме се фајл брише тридесет и осам пута (толико одштампа и звездаца *), и не можете га наћи ни у кантици за смеће, нити га можете повратити. Наравно, ово може трајати дуже, што зависи од величине фајла који се преписује новим садржајем. Код *срм*-а је подразумевано сигурно брисање, и ако не наведете неке друге опције, фајл се пребрише тридесет и осам пута новим садржајем. Могуће је такође користити и брзо несигурно брисање навођењем опције *f* која не укључује преписивање насумичног садржаја преко оригиналног фајла тридесет и осам пута, или тотално несигурно брисање од само два пута ако наведете опцију *l*.

Трећи програм за сигурно брисање под ГНУ/Линукс оперативним системима би био Вајп (енг. *wipe*). Њега можете инсталирати на следећи начин:

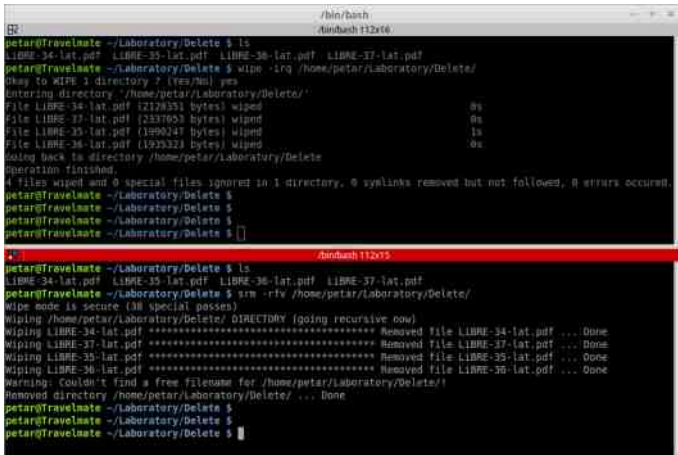
```
sudo apt-get install wipe
```

Веома сличан са *срм*-ом, Вајп преписује нови садржај тридесет и пет пута преко оригинала, али се после навођење опције *-q -Q* може одредити број пута преписивања новог насумичног садржаја преко оригинала.

Како да...?



Још једна сличност са `srм`-ом је да се може задати цео директоријум употребом опције `r`, после које се задаје путања до директоријума из кога ће бити обрисани сви фајлови и сви субдиректоријуми рекурзивно.



Уколико желите графички приказ (*GUI*), односно да имате ову опцију за сигурно брисање фајла доступну само једним кликом, можете инсталирати Вајпов додаток за фајл менаџер Наутилус командом:

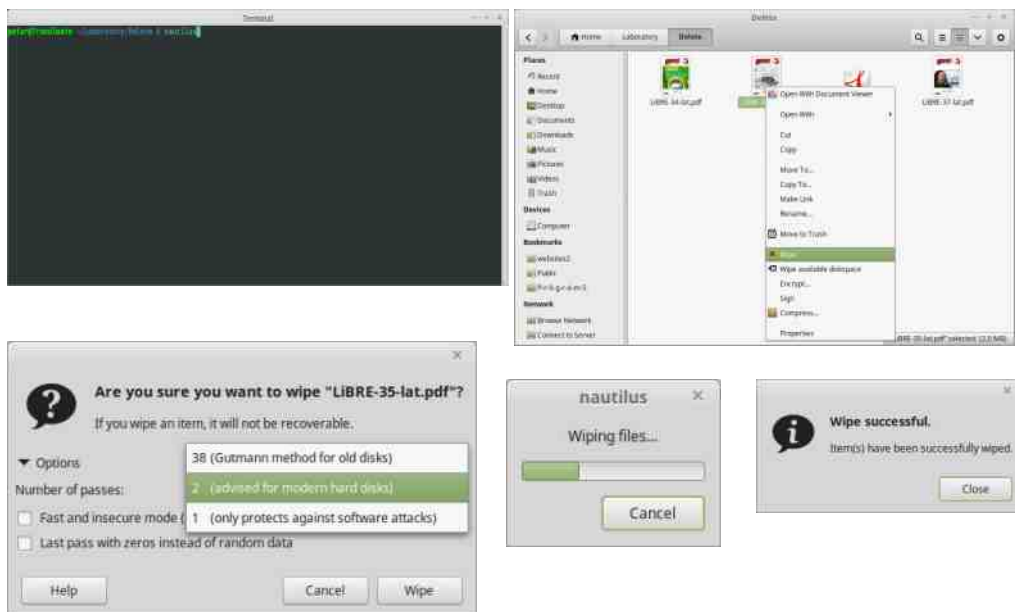
```
sudo apt-get install nautilus-wipe
```

Тада можете покренути Наутилус и из удобности фајл менаџера и навигације мишем, само једним десним кликом на фајл одабрати опцију за његово сигурно брисање. Само имајте на уму да је оно подразумевано подешено на две итерације преписивања садржаја за модерне дискове, што лако можете променити у



Сигурно брисање података

простору који се отвара пре брисања фајла на тридесет и осам преписивања за параноичне.



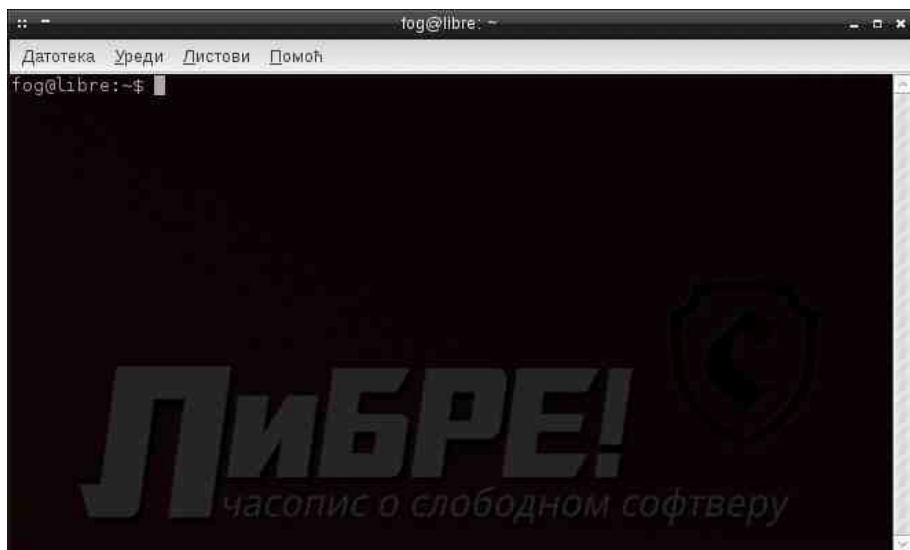
Наравно, ту је и Блич-бит, (енг. *BleachBit*) (<http://goo.gl/uOep>) програм отвореног кода који није објављен под Општом јавном лиценцом. Он за вас осим брисања фајлова може урадити још многа корисна чишћења непотребних података у целом рачунару, па је свакако препоручено и њега користити. Овај програм је намењен и за оперативни систем Виндоуз, док је ту и програм Брисач (енг. *Eraser*) (<http://goo.gl/dYL7>). Објављен је под Општом јавном лиценцом и намењен је само корисницима Виндоуза. За кориснике Мек ОС X постоји програм отвореног кода „Трајни брисач“ (енг. *Permanent Eraser*) (<http://goo.gl/1aQOr>) који имплементира Гутманову методу преписивања. Постоји и оперативни систем намењен за сигурно брисање или боље речено, уништавање података под називом **ДБАН** (енг. *Darik's Boot and Nuke*) кога можете преузети са адресе <http://www.dban.org/>.

У следећем делу ћемо се више позабавити флеш и оперативним меморијама као и своп партицијама, а изложићемо и кратак опис и упутство за коришћење ДБАН диска.

Команде у ГНУ/Линуксу (1. део)

Аутор: Данијел Гомола

У овој теми позабавићемо се основама Линуксовог командног окружења. Приказаћемо основне команде које се користе у свакодневном раду у Линуксу. Ово је тек први део, али је за почетак сасвим довољан за кориснике који су нови у Линуксу. Пре свега, морате знати у чему се и како се извршавају команде. Команде се могу извршавати у текстуалном или графичком интерфејсу оперативног система (енгл. *GUI*) уз помоћ апликације која долази уз Линукс дистрибуције – терминал. У терминалу се команде извршавају када се појави тзв. позив за унос у облику доње црте (`_`), као на слици испод, и унесе назив команде коју желимо да извршимо.





Најчешће коришћене команде

Ако сте схватили где се и на који начин се извршавају команде, онда се можете упознати и са командама које се врло често користе. Команди има много. Но, чак и напредни корисници Линукса користе само оне које се најчешће користе. Зато ћемо објаснити управо такве команде.

su

Команда *su* је једна од основних команди и корисна је у многим ситуацијама. Обично се користи за прелазак међу обичне кориснике или између обичног корисника и суперкорисника (енгл. *root*). Ова опција је много лакша него да се одјављујете са једног корисничког налога па да се пријављујете поново на други. Овом командом можете се пријавити као други корисник без одјављивања са тренутног налога. Једини проблем је у томе што, ако хоћете да се пријавите одједном као два корисника у терминалу, морате да користите два прозора. Проблем се решава тако што се пријавите као други корисник па, кад завршите са радом као тај корисник, командом *exit* враћате се на првог корисника.

Када хоћете да се пријавите као други корисник, онда ћете уписати следеће:

```
su korisnik2
```

Наравно, уместо *korisnik2* куцате име корисничког налога на који желите да се пријавите.

Затим, ако је постављена лозинка на тај кориснички налог, тражиће од вас да упишете лозинку.

```
su korisnik2  
Password:
```

Лозинка коју будете куцали неће се приказивати. Када је откуцате, само притисните Ентер и бићете уловани. Кад вам више не буде требао тај налог, можете се лако одјавити командом *exit*.

```
exit
```

Ако желите да се пријавите као администратор тј. суперкорисник, онда само

Ослобађање

откуцајте команду `su` .

```
su  
Password:
```

Откуцајте лозинку суперкорисника.

`pwd`, `cd`, `ls`

Ове команде су основне команде за рад са датотекама.

Наредба `pwd` приказује у ком се директоријуму тренутно налазимо.

```
pwd  
/home/danijel
```

Вама ће исписати други директоријум где се налазите у тренутку извршавања ове команде. Ако хоћете да промените директоријум, можете откуцати комаду `cd` да бисте прешли у други директоријум. То изгледа овако:

```
cd Pictures
```

Ви уместо `Pictures` куцате друго одредиште у које желите да се пребаците. Сада можете проверити командом `pwd` да ли сте се пребацили у директоријум који сте желели. Најзад, командом `ls` можете приказати шта се налази у жељеном директоријуму.

```
cd Pictures  
~/Pictures $ ls  
Tux.png Tux_Wallpaper.png
```

Уколико желите да излистате податке који се налазе у неком другом директоријуму, онда само откуцајте `ls` Име_Директоријума.

Сада знате како функционишу команде `pwd`, `cd` и `ls`.



Команде у ГНУ/Линуксу

gzip

Командом `gzip` можете да запакујете тј. архивирате неки фајл у `.gz` формат.

```
gzip spisak.txt
```

Да бисте распаковали фајл, куцајте:

```
gzip -d spisak.txt.gz
```

Ово су само основне функције команде `gzip`.

Надамо се да сте схватили функције свих команди наведених у овом тексту. Ово је сасвим довољно за почетак. У наставку ове теме ћемо упоредити разна командна окружења и погледати како функционише командно окружење Баш (енг. *Bash*).



I ❤️ #!/bin/bash

Преглед популарности ГНУ/Линукс и БСД дистрибуција за месец август

Distrowatch

1	Mint	2983<
2	Debian	2176>
3	Ubuntu	1535>
4	openSUSE	1324>
5	Manjaro	1187>
6	Fedora	1168>
7	Kali	974>
8	Mageia	968>
9	CentOS	921<
10	LXLE	832>
11	Arch	776>
12	Lite	720<
13	elementary	665>
14	PCLinuxOS	616>
15	Zorin	614<
16	Android-x86	569>
17	Puppy	563>
18	Lubuntu	548<
19	Bodhi	531<
20	KaOS	529<
21	Robolinux	509>
22	FreeBSD	482<
23	Q4OS	474=
24	Ubuntu MATE	473>
25	Tails	457=

Пад <
 Пораст >
 Исти рејтинг =
 (Коришћени подаци са Дистровоча)

Ваш посао, опен-сорс посао (5. део)

Мозила — Од заједнице до корпорације



Аутор: Дејан Маглов

У прошлом броју смо вас подсетили на почетке развоја слободног софтвера. Манифест ГНУ-а је основни документ и главни законик за слободан софтвер. Он прописује шта је морално наплатити код слободног софтвера. Свако ограничење које не поштује смернице из манифеста ГНУ-а издваја тај софтвер из оквира слободног софтвера и сврстава га у категорију власничког софтвера (комерцијални или фривер), или, ако има слободан код, у категорију опен-сорс.

Суштина јесте да софтвер буде слободан за проучавање, измене, унапређење и даље дељење. Нигде не пише да се слободан софтвер не може продавати; једино се не сме ни на који начин забранити његова даља слобода. Због овог правила се слободан софтвер практично може продати само једном јер већ следећи корисник може да направи неограничен број копија које сме да подели бесплатно. Зато се код слободног софтвера увек комерцијализује неки други сегмент који није везан за сам софтвер, као што су прилагођавање заинтересованом кориснику, одржавање, техничка подршка и едукација.



Када интернет није био толико развијен, софтвер је био дистрибуиран поштом. То је омогућавало малу зараду, јер је поред поштарине дистрибутер могао да наплати и малу надокнаду за прављење копије и медиј. Савремени интернет је ту могућност ускратио, али је донео нове могућности. Нарочито у САД је



убичајна пракса да се може наплатити препорука за одређене интернетске локације. Један од првих великих таквих интернетских локација био је АОЛ (енг. *America Online* - Америка онлајн). АОЛ је међу првима понудио вести, забаву и комерцијалне садржаје на једном месту и од интернета је направио бизнис. Као такав је имао интереса да спонзорише препоруке за свој садржај. Јаху (енг. *Yahoo*) је један од првих савремених интернетских претраживача. Јаху је глобализовао интернет да би Гугл (енг. *Google*) данас од интернета направио „глобално село”. Сви ови велики играчи имају интереса да понуде новчану надокнаду за рекламирање својих садржаја и услуга. Ово је прилика да произвођачи софтвера продају рекламу уместо софтвера.

YAHOO! Google

Ову ситуацију користи и власнички фривер (бесплатни софтвер) додајући агресивне рекламе уз софтвер који нуде корисницима, али и слободни софтвер. Једина разлика је што је код слободног софтвера могуће избацити делове кода који се односе на рекламу.

Мозила, корпорација, профит?

Пре неколико месеци смо били сведоци наизглед безначајне информације да је слободни интернетски прегледач Фајерфокс променио подразумевани интернетски претраживач. Са до тада подразумеваног Гугла прешао је на Јаху. Ншта драматично се није десило; корисник и даље може сам да промени подразумевани претраживач и користи онај који је њему најзгоднији, тј. онај на који је навикао.



Слободни професионалац

Пошто знамо да иза Фајерфокса стоји профитабилна фирма Мозила корпорација (енг. *Mozilla Corporation*) са преко хиљаду стално запослених и да су осим Фајерфокса њени производи такође потпуно слободни софтвери (попут Тандерберда и Симанкија), поставља се питање: одакле профит?

Мозила је првенствено пројекат на који се могу угледати многи други пројекти слободног софтвера. Мозила је настала као заједница (енг. *community*) окупљена око људи који су радили на Нетскејп Навигатору, интернетском прегледачу који је био веома популаран у то време и који је био једини озбиљни конкурент Мајкрософтовом Интернет Експлореру на персоналним рачунарима. „Заражени” вирусом филозофије слободног софтвера објављују опен-сорс верзију Нетскејп Комуникатора.

У почетку је Мозила била под окриљем већ поменутог АОЛ-а који је стајао иза пројекта Нетскејп. После драстичног смањења удела АОЛ-а у пројекту Мозила, заједница оснива 2003. године непрофитну Мозила фондацију са циљем правне заштите пројекта и боље координације рада заједнице. Овај потез осигурава преживљавање пројекта без учешћа АОЛ-а. Када се указала могућност да пројекат буде профитабилан, Мозила фондација оснива профитабилно предузеће Мозила корпорацију 2005. године.



Мозила корпорација прераста у предузеће са више од хиљаду стално запослених радника и приходом од преко три стотине милиона долара годишње. Осамдесет пет посто укупних примања долази из уговора Мозиле са подразумеваним претраживачем. То је раније био Гугл, а од недавно је то Јаху.



Како и зашто ово функционише?

Зашто би Гугл, или сада Јаху, дали оволики новац само због једног подешавања у Фајерфоксу, који се лако може променити по жељи корисника? Ово вероватно и не би функционисало ван америчког тржишта, али срећом по Мозилу америчко тржиште је велико.

Сваки просечни Американац је навикнут на две ствари. Прва је да има на сваки производ гаранцију за поврат новца. То значи да, уколико у року до петнаест дана уочи било какав недостатак на производу, може без икаквог образложења да врати производ трговцу и да добије своје паре назад. Услов за то је да не постоји никаква видљива промена на производу. Чак и промена подешавања може да буде разлог за одбијање рекламације. Након ове гаранције почиње да тече и гаранција коју сви познајемо - на техничку исправност производа у одређеном року. И у том року може да нам буде одбијена рекламација због неког нашег подешавања производа. Због свега овога просечан Американац врло ретко врши своја подешавања чак и кад је то дозвољено. Задовољава се функционисањем производа „аут оф бокс“ (енг. *out of box* - фабричка подешавања), или користи право гаранције за поврат новца.

Слободни професионалац

Зато су Американцима врло важна фабричка подешавања, а то је разлог што се и ФЛОСС заједница жали на произвођаче хардвера што ретко прединсталирају слободан софтвер на своје производе. Да то чешће чине, барем у Америци би популарност слободног софтвера била већа.

Комбинација навика просечних Американаца и прилично велике популарности Фајерфокса као интернетског прегледача је омогућила Мозила солидан приход на основу уговора са главним интернетским претраживачима. Није им то једини приход, али јесте главни.

Закључак

Мозила је добар пример како од обичног опен-сорс пројекта доћи до комерцијализације слободног софтвера. Развој им је веома логичан и примењив на друге опен-сорс пројекте. Као прво, нису почели од нуле, него од већ популарног производа са потпором већ озбиљне фирме (АОЛ). На време су се осамосталили од АОЛ-а, кад је он престао да буде „озбиљан играч“ у свету интернета, преко непрофитне организације Мозила фондације која им је омогућила правну сигурност. Тек на крају, пошто се указала прилика за комерцијализацију пројекта, захваљујући доброј организацији Мозила фондације, лако оснивају Мозила корпорацију која преузима послове комерцијализације пројекта.

Пут је веома логичан и примењив на просторима ван Америке. Додуше, тешко је да се ико мери са популарношћу Фајерфокса и немамо Гугл да подржи неке од наших пројеката, али принцип се може копирати.



mozilla
CORPORATION



Шифровани чет (4. део)



Аутор: Петар Симић

Увод

Сагу о програмима за сигурно, или је можда боље рећи „за сигурније“ ћаскање настављамо новим програмом из ове бранше, а који је прави плод масовнијег размишљања о приватности које нам доноси доба после Сноудена.

Програм користи ДХТ (Дистрибуиране хеш табеле) за проналажење и повезивање са другим корисницима, што га чини децентрализованим програмом јер се заснива на дистрибуираној мрежи и протоколима, па самим тим отпорним је и на цензуру. Програм је, наравно, отвореног кода и објављен је под Општом јавном лиценцом треће верзије. Код можете пронаћи на следећем Гитхабу (<https://goo.gl/GTB93Z>).

Технички део

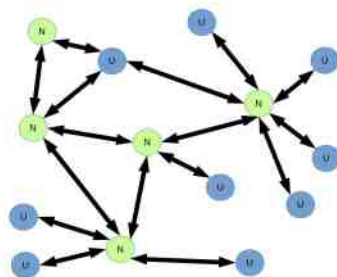
Као што га и сами аутори описују, Токс (*Tox*) је слободан, п2п (*peer-to-peer*), дистрибуиран, Е2ЕЕ (*End-to-End Encrypted*) шифрован од једног до другог краја, мултимедијални програм за сигурну видео, аудио и текстуалну комуникацију. Од самог тренутка лансирања овог програма, сматра се и добром и слободном алтернативом Скајпу.

Пошто је мрежа дистрибуирана и налик на друге п2п мреже, не постоји један централни сервер од којег она зависи. Међутим, он није ни потпуно децентрализован, као што то нису ни торенти, јер је потребно имати неко

Интернет мреже и комуникације

централно место са кога ћете их пронаћи као што је Пајрат-беј (*ThePirateBay*). Исти принцип важи и овде - мрежа се састоји од нодова (чворова), који повезују кориснике, и корисника. Нодове такође покрећу корисници и свако може бити нод и додати свој нод у главну јавну листу (<https://goo.gl/HNB74D>).

Ако знате да Тор мрежа функционише на принципу добровољаца, онда ће вам бити лако да схватите и начин функционисања Токс мреже. Нодови служе за проналажење корисника у Токс мрежи и повезивању корисника, па су самим тим и посредници у међусобној комуникацији самих корисника.



При првом покретању програма после инсталације Токс ће за вас креирати јединствени ИД који се састоји од слова и бројева и који заправо представља вас у мрежи. ИД је нека врста хешираног асиметричног кључа који се користи за шифровану комуникацију између корисника - или је чак и сам јавни кључ.

Када се каже да је комуникација шифрована од једног до другог краја, мисли се на асиметрично шифровање са јавним и тајним кључевима, попут оног за електронску пошту. Користи се модерно ЕЦЦ (*Elliptic Curve Cryptography, curve25519*) шифровање помоћу елиптичких кривих за размену кључева, и **xsalsa20** за само шифровање, и **poly1305** за аутентификацију (MAC) из *NaCl* библиотеке. Због овога је немогуће фалсификовати ваш идентитет у мрежи, осим ако се неко не домогне вашег тајног кључа. Да су аутори мислили о свему, говори и чињеница да се користи и OTP (Off-The-Record) вид заштићене комуникације који гарантује криптографску независност међусобно размењиваног шифрованог садржаја. Ово у преводу значи да уколико неко успе да дешифрира једну од комуникација, то му ништа не говори о другим, јер се за сваку нову комуникацију користи нови пар кључева који се по завршетку комуникације одбацује. Такође ваља рећи да нема нешифроване комуникације - свака врста комуникације се



обавезно и увек шифрује пре него што напусти Токс програм, односно пре него што се пошаље у Токс мрежу.

Инсталација

Иако Токс има сличне клијенте за већину оперативних система или платформи као што су Виндоуз, Мек ОС десет, Линукс, БСД, Андроид и иОС, овде се бавимо само инсталацијом и подешавањима за Линукс, тачније у даљем опису је наведен пример инсталације на Линуксу заснованом на Дебијану (Убунту, Лубунту, Зубунту, Минт и сличним).

Најпре је потребно отићи на њихов сајт и у делу за преузимање клијената на адреси (<https://goo.gl/2F6uG9>) преузети жељеног клијента. Овде имате избор између клијената са и без графичког окружења (ГУИ), као што су Ратокс (Ratox) и Токсик (Toxic), као и ужи избор унутар оних са графичким окружењем као што су Блајт (Blight), Јутокс (uTox) и Кјутокс (qTox).

Аутор је у наставку описао процес инсталације и подешавања за Кјутокс због очигледних предности над Јутоксом наведених на њиховом сајту (<https://wiki.tox.im/Client>), али ако се пак одлучите за Јутокс, инсталација и покретање су врло слични, док инсталацију клијената без графичког окружења аутор овог теста није испробао па она овде није описана, али се може наћи на њиховом сајту.

На претходно поменутој локацији за преузимање клијената имате опет две могућности: или да једноставно скинете запаковану архиву у **.xz** формату, распакујете и покренете програм без инсталације само ради пробе и тестирања - или да, пак, инсталирате програм на вашој машини. За инсталацију је потребно покренути следеће комаде из терминала

```
sudo apt-key del 0C2E03A0
sudo sh -c 'echo "deb https://repo.tox.im/ nightly main" >
/etc/apt/sources.list.d/tox.list'
wget -qO - https://repo.tox.im/pubkey.gpg | sudo apt-key add -
sudo apt-get install apt-transport-https
sudo apt-get update -qq
sudo apt-get install qtox
```

Интернет мреже и комуникације

које се такође налазе и код њих на сајту, или, ако сте помало хакер и мрзите да откуцавате команде и чекате да одраде своје, можете да на брзину напишете просту шел скрипту са овим командама која ће све наведено већ урадити за вас. Пример једне такве шел скрипте је:

```
#!/bin/bash
#remove old key
sudo apt-key del 0C2E03A0
sudo sh -c 'echo "deb https://repo.tox.im/ nightly main" >
/etc/apt/sources.list.d/tox.list'
wget -qO - https://repo.tox.im/pubkey.gpg | sudo apt-key add -
sudo apt-get install apt-transport-https
sudo apt-get update -qq
echo "Tox Repository Installed." echo "You can now install utox,
qtox, toxic, ratox and tox-bootstrap
sudo apt-get install qtox
```

Наравно, покретање шел скрипте из фолдера где сте је сачували са екстензијом **.sh** иде из терминала

```
sudo sh ime_skripte.sh
```

Након овога је Токс клијент инсталиран и можете га покренути из терминала или га потражити међу инсталираним програмима на вашој машини.

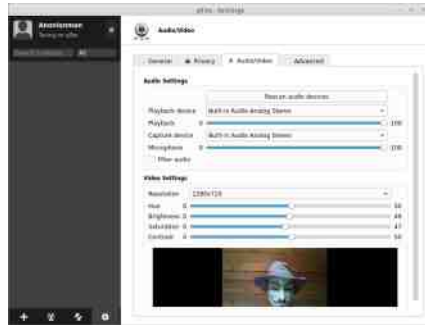


Подешавања

Сада је потребно да имате камеру и микрофон прикључене на рачунар и да их

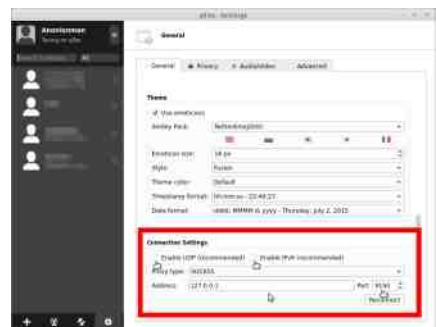


тестирасте:



Пошто су сва подешавања већ намештена, све нормално функционише после инсталације, али уколико желите, програм моћете да прилагодите својим потребама, ако знате шта радите. Треба напоменути и да су аутори Токса мислили и о употреби њиховог програма преко Тор анонимне мреже за виши ниво безбедности и приватности корисника и њихових комуникација. Ако сте један од оправданих параноика пост-Сноуденове ере и желите да испробате Токс преко Тора, то можете учинити на следећи начин:

Прво је потребно да у подешавањима за мрежу која се налазе на дну генералних подешавања подесите да се **НЕ** користе *UDP* и *IPv6*, и да се користи *SOCKS5* прокси на вашој локалној адреси *127.0.0.1* и порт је *9050* ако сте покренули инсталирани Тор на рачунару или *9150* ако сте покренули портабилни Тор преко ТББ (*Tor Browser Bundle*) преко њиховог претраживача Фајерфокс.



Подешавања је затим потребно сачувати и рестартовати Токс како бисте били сигурни да су сва подешавања прихваћена, док Тор мора остати функционалан за

Интернет мреже и комуникације

то време како би Токс успео да се повеже преко ове анонимне мреже. О овоме можете сазнати и на њиховој веб-страни посвећеној подешавању за употребу са Тор мрежом на <https://goo.gl/GHgam9>

Сада сте спремни за анонимну шифровану комуникацију.

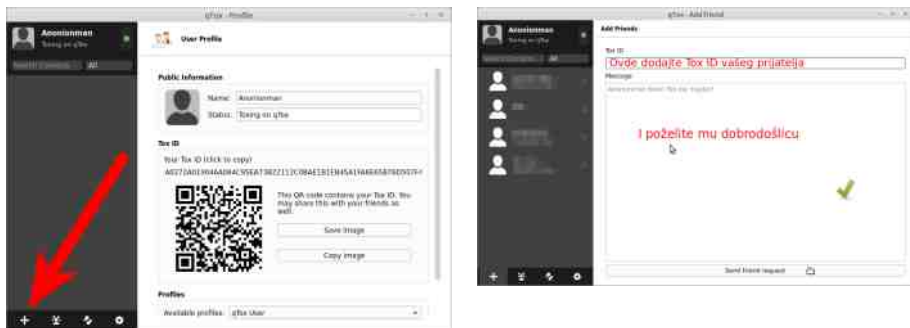
Умрежавање

Да бисте се повезали са другим корисником ове мреже, потребно је да размените ТоксИД идентификације, тј. морате знати ИД другог корисника или да он зна ваш да бисте се повезали. О начину на који ћете разменити ИД-еве са неким сами одлучујете, а савет аутора овог текста је да се то изведе шифрованом поштом.

Када додате пријатеља, он ће се појавити у левом делу програма у листи са контактима, и имаће нотификацију као доступан (зелени пун кружић) или одсутан (празан црвени кружић).

Токс подржава и размену фајлова и групни чет који се још увек развија.

Мрежи можете допринети и покретањем једног нода као и у случају Тор анонимне мреже, чиме истовремено доприносите својој заштити јер је страном посматрачу тада теже да каже када ви користите Токс мрежу на том ноду, а када тај нод само прослеђује туђе поруке.



Овај програм није усамљен и већ постоји сличан програм по имену Ринг (<http://ring.cx/>), који још није у потпуности функционалан и још увек је у раним фазама развоја, али се надамо да ће стећи већу популарност и функционалност до краја наше саге о програмима за шифровани чет.



Облаци и катанци:

Сигурни у облацима (1. део)



Аутор: Петар Симовић

Клауд технологија се развија већ неко време и дуже од десет година постоје разна решења. Ова технологија подразумева употребу удаљеног рачунара или виртуелне машине на неким удаљеним серверима уместо сопствене машине за обављање израчунавања или чувања података. Као и код друштвених мрежа, у употреби су и разна решења чувања података у облаку, од којих опет нека имају и бесплатне варијанте.

Шта се заиста дешава у облаку, где се физички чувају наши подаци и ко све има приступ њима – тешко је рећи. То подиже ниво сумње и скепсе када је у питању употреба ове корисне и делом бесплатне технологије, као и решења разних компанија које се заснивају на примени ових и сродних технологија. Многе компаније нуде разна решења у облику јавних и приватних облака, софтвера као услуге (SAAS - *Software as a service*) те читавих платформи (PAAS - *Platform as a service*), од којих је најпознатија компанија Амазон. Не морамо бити укорок са најновијим технологијама како бисмо разумели начин функционисања ове технологије. Заправо, мејл сервисе и многе старије познате технологије као што су ВПС (*Virtual Private Server*), ВПН (*Virtual Private Network*), ВНЦ, ССХ и ФТП

Интернет мреже и комуникације

можемо посматрати као старија и примитивнија решења од PAAS или SAAS технологија и њиховим неопходним претходницама у развоју.



Међутим, већина софтвера који омогућавају laku употребу ових технологија је затвореног кода, па им је због тог разлога тешко веровати.

И ту, заправо, долазимо до суштине и кључног питања:

„Да ли се морамо одрећи своје приватности да бисмо користили нове, привлачне и корисне технологије?”

Иако одговор може да варира зависно од конкретне технологије на коју се оно односи, у нашем случају употребе складишног простора на облаку, била она бесплатна или не, насрећу је негативан.

Ситуација је интересантна и из другог угла, када се поставља питање које сте вероватно и сами себи поставили при сусрету са новим апликацијама за мобилне телефоне као што су, на пример, Вотсап (*Whatsapp*), Вајбер (*Viber*), Инстаграм и друге:

„Како се компанијама исплати да нам дају пет, десет, педесет, сто или чак хиљаду некаквих гигабајта бесплатно? Сервери на више локација, бекап и редувантност, инсталација, одржавање, струја, запослени, чак и домен коштају много, а нама се услуга даје џабе”.

Па, једноставан одговор гласи да се информације о нама продају. Било да су те информације заправо стварни сирови садржај који користимо на нечијем диску или пак метаподаци (подаци о подацима, види број 26), свака информација о нама се вреднује и продаје на тржишту.



Како бисте лакше ово разумели, рецимо да упознате неку особу уживо или на друштвеним мрежама и хоћете да сазнате што више или све о тој особи. Колико бисте платили да само сазнате какве податке та особа има, рецимо, на Дропбоксу, без увида у њих? Шта мислите, колико бисте платили да стварно имате комплетан увид у те податке или копију?

Ово је такође занимљив феномен где **бесплатне услуге плаћамо одавањем приватних и личних информација**. Имајте ово на уму када будете инсталирали нову апликацију на паметним телефонима и када прихватате услове коришћења без читања истих. Да бисте се у ово лично уверили, погледајте барем неке од седам кратких епизода из серијала **Do Not Track** са сајта <https://goo.gl/m0NVP8> Како бисмо ипак користили погодности бесплатног бекапа, а истовремено сакрили своје податке и метаподатке, користимо енкрипцију, односно шифровање. Знамо да то није ништа ново нити је било тешко погодити, али овде ћемо се озбиљније позабавити овим проблемом и предлагати параноична решења која минимизују „цурење“ ваших података са вашег приватног рачунара.

Зависно од одабира провајдера складишног простора у облаку, тј. од тога да ли се за регистрацију захтева остављање имејл-адресе, потребно ју је имати. Иако свако од нас сигурно има бар једну, овде ће нам требати анонимна имејл-адреса која нема ничега заједничког са вама и ни на који начин не повезује баш вас са собом. Ово је пожељно али не и неопходно како бисмо при регистрацији, која ће такође бити анонимна, провајдеру оставили што мање информација о томе ко смо заправо ми и за шта користимо простор који нам нуди. Ово је само увод, а у следећем делу ћемо проћи кроз процес креирања анонимне имејл-адресе и налога за услугу складишног простора у облаку, као и кроз процес инсталирања и подешавања бесплатног анонимног бекаповања података на облак.



Dropbox

BALCCON2015

Balkan Computer Congress

11|12|13 September

Novi Sad, Serbia

<https://balcon.org>

LUGONS
Linux User Group of Novi Sad

Hack

Play

Learn

Socialize

W
HOLLAND
STIFTUNG