CARNET

Tor Browser

NCERT-PUBDOC-2017-11-348

CERT.hr

Sadržaj

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

1 Uvod

Kako bi bilo moguće razumjeti korist i svrhu Tor Browser-a, nužno je razumjeti što je to **Tor**. Tor je **mreža anonimnosti** koju svi korisnici Interneta mogu koristiti za veću anonimnost i privatnost na Internetu. Kada je korisnik spojen na Tor, njegov mrežni promet višestruko je šifriran te usmjeren kroz mrežne čvorove diljem svijeta prije dolaska na svoje odredište. Na taj se način sadržaj mrežnog prometa štiti, a njegov mrežni put prikriva kako bi se **otežalo prisluškivanje prometa i otkrivanje njegovog izvora odnosno odredišta**.

1.1 Za koga je Tor namijenjen?

Tor je originalno nastao kao projekt ratne mornarice SAD-a sa svrhom zaštite mrežne komunikacije institucija SAD-a, no danas ga koristi velik broj različitih korisnika:

- od novinara, aktivista i zviždača (eng. *whistleblowers*) kojima je nužna tajnost njihove komunikacije,
- preko policije i vojske koji žele sakriti svoje istrage od osumnjičenika odnosno prikriti svoje operacije od neprijatelja,
- do građana koji žele zaobići cenzuru ili samo koristiti Internet anonimno i privatno.

Bitno je razumjeti da građani imaju pravo anonimno i privatno komunicirati, te da im za to nije potreban nikakav poseban razlog. Reporteri Bez Granica, internacionalna neprofitna i nevladina organizacija koja promovira i brani slobodu medija i pristupa informacijama, preporuča korištenje Tor mreže za zaobilaženje cenzure i osiguravanje komunikacije i podataka kao dio „kompleta za preživljavanje na mreži“ (eng. *online survival kit*).

Tor mreža dostupna je svima, sve što je potrebno za njeno korištenje je računalo, veza na Internet i slobodno dostupni alati. Čak i za građane koji trenutno nisu zabrinuti za privatnost svoje komunikacije, znanje kako koristiti Tor mrežu može biti korisno u budućnosti.

1.2 Kako Tor mreža funkcionira?

Tor mreža primarno se sastoji od **brojnih volonterskih računala** kroz koje se usmjerava mrežni promet korisnika.

Prilikom spajanja na Tor, računalo korisnika odabire tri volonterska računala Tor mreže. Korisnikovo računalo pokušava odabrati tri volonterska računala koja su **neovisna** jedno o drugome (ne pokreće ih isti volonter, ne nalaze se u istoj državi …). Njihova neovisnost ključna je za očuvanje anonimnosti te će njen značaj postati jasan kasnije.

Nakon odabira volonterskih računala, korisnik može započeti s korištenjem Tor mreže. Slika 1 prikazuje kako je korisnikov mrežni promet (prikazan kao poruka) zaštićen i kako on putuje kroz Tor mrežu:

1. Jednom kada korisnik želi poslati poruku nekom računalu na Internetu, on tu poruku **slojevito šifrira** – prvo ju šifrira za treće (na slici plavo) odabrano volontersko računalo, zatim rezultat toga šifrira za drugo (ljubičasto) odabrano računalo i konačno rezultat toga šifrira za prvo (žuto) odabrano računalo.

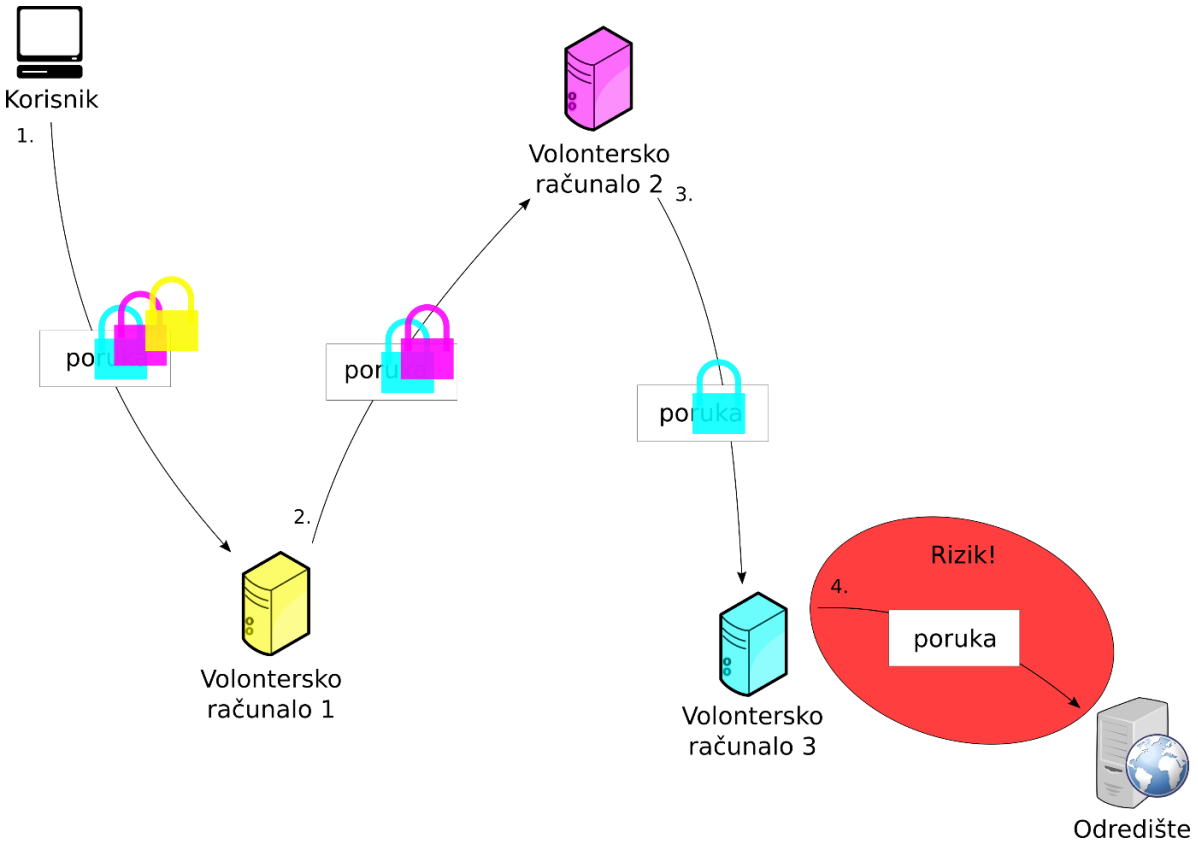
   Na slici su te šifre prikazane kao plavi, ljubičasti odnosno žuti lokot i odgovaraju bojama volonterskih računala koja ih mogu dešifrirati. Ovako slojevito šifriranu poruku sada je moguće u potpunosti dešifrirati samo tako da ju prvo dešifrira prvo (žuto) volontersko računalo, zatim drugo (ljubičasto) i konačno treće (plavo).

   Šifriranu poruku sada korisnik šalje prvom volonterskom računalu.

2. Prvo volontersko računalo prima slojevito šifriranu poruku, dešifrira vanjski sloj („uklanja“ žuti lokot) i šalje rezultat drugom volonterskom računalu.

3. Drugo volontersko računalo prima tu poruku, dešifrira još jedan sloj („uklanja“ ljubičasti lokot) i šalje poruku trećem volonterskom računalu.

4. Treće volontersko računalo prima tu poruku, dešifrira zadnji sloj („uklanja“ plavi lokot) i šalje poruku odredištu. U ovom trenutku poruka **izlazi iz Tor mreže** i završava na odredišnom računalu.



Slika 1 - put prometa kroz Tor mrežu

Prednost ovog pristupa je što svaki čvor na mrežnom putu samo zna od koga je primio poruku, i kome je prosljeđuje – ništa drugo:

- Prvo volontersko računalo samo zna da je primilo nekakvu poruku od korisnika i da ju treba usmjeriti drugom računalu – ne zna što ta poruka sadrži ni gdje joj je konačno odredište.

- Drugo računalo zna da je primilo poruku od prvog računala i da ju treba usmjeriti trećem računalu – ali ne zna da je ta poruka originalno došla od korisnika, niti zna koji je njen sadržaj ni koje joj je konačno odredište.

- Treće računalo zna da je primilo poruku od drugog računala, **zna sadržaj te poruke** (ako on nije dodatno zaštićen) i da ju treba poslati na konačno odredište – ali ne zna da je ta poruka došla od korisnika niti da je došla preko prvog računala.

    - Na Internetu je uvijek bitno **koristiti zaštićene mrežne protokole**, kao što je HTTPS, umjesto nesigurnih, kao što je HTTP. Neovisno o tome koristi li se Tor mreža ili ne – **postojat će računala** na mrežnom putu koja će **moći pročitati poruke** koje korisnik šalje ako one nisu dodatno zaštićene. Na slici 1, ovaj rizični dio mrežnog puta označen je crvenom elipsom i natpisom „Rizik!".

      Korištenjem zaštićenog protokola kao što je HTTPS, poruka je šifrirana na računalu korisnika i dešifrira se tek na krajnjem odredištu (eng. *end-to-end encryption*), i zbog toga nije čitljiva nikome po putu, pa tako ni (u slučaju Tor mreže) trećem volonterskom računalu.

- Odredišno računalo **ne zna od koga je primilo poruku** (samo zna da ju je treće računalo prenijelo) – osim naravno ako se to može iščitati iz samog sadržaja poruke.

Ako su odabrana volonterska računala **neovisna** i ne dijele informacije, neće postojati nitko tko u isto vrijeme zna i **tko je poslao** poruku i **kome je ona namijenjena**.

Ovaj cijeli proces naziva se slojevito usmjeravanje (eng. *onion routing*) i izrazito dobro sakriva tragove mrežnog prometa. Samo ime Tor je zapravo nastalo kao skraćenica od eng. *The Onion Router*, što se može prevesti kao slojeviti usmjerivač. Sada, nakon uvodnog objašnjenja Tor mreže, moguće je objasniti korist i svrhu Tor Browser-a.

2 Tor Browser

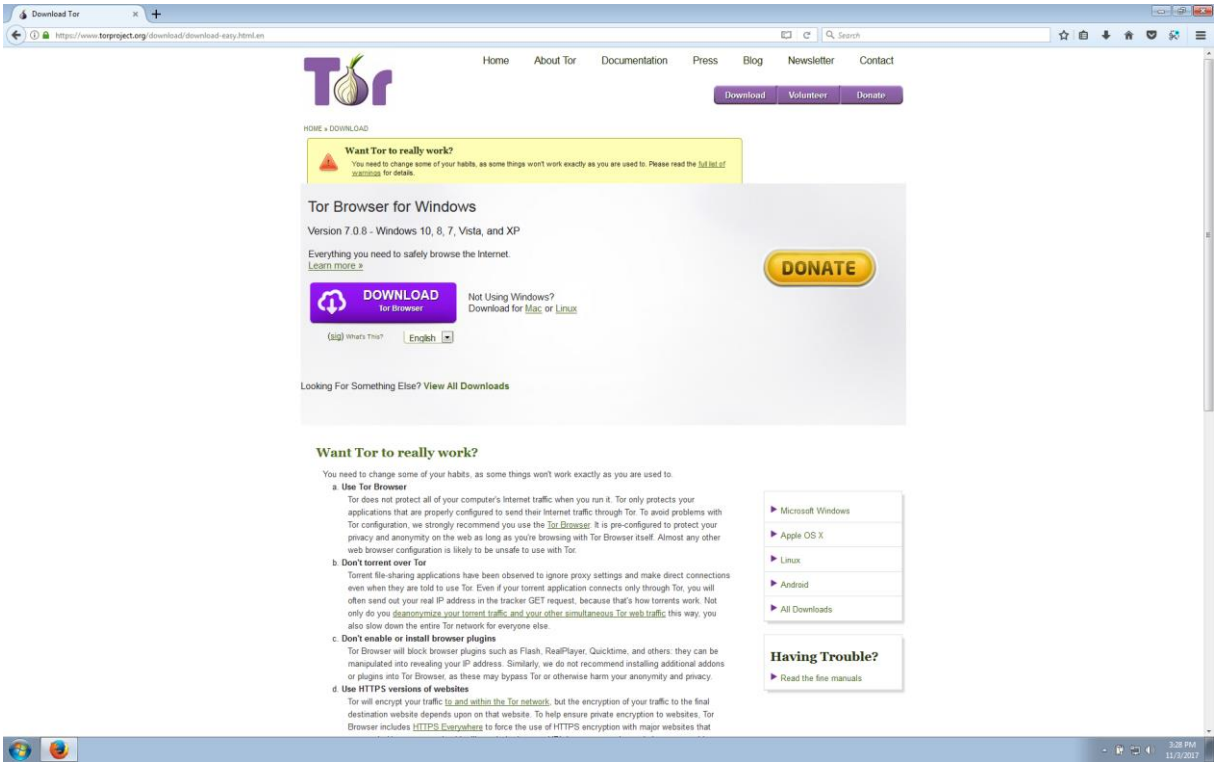
Kao krajnji korisnik, najlakši način za korištenje Tor-a za anonimnost i zaštitu svoje privatnosti je **Tor Browser (Tor Web preglednik)**. To je programski paket koji sadržava sve što je potrebno krajnjem korisniku da pregledava Web putem Tor-a.

Iz perspektive korisnika, to je zapravo samo **poseban Web preglednik** (temeljen na *Mozilla Firefox*-u) koji **koristi Tor mrežu** i sadrži dodatne zaštite. Tor Browser je dostupan za Microsoft Windows, Apple OS X i Linux te postoji i posebna inačica za Android pametne telefone.

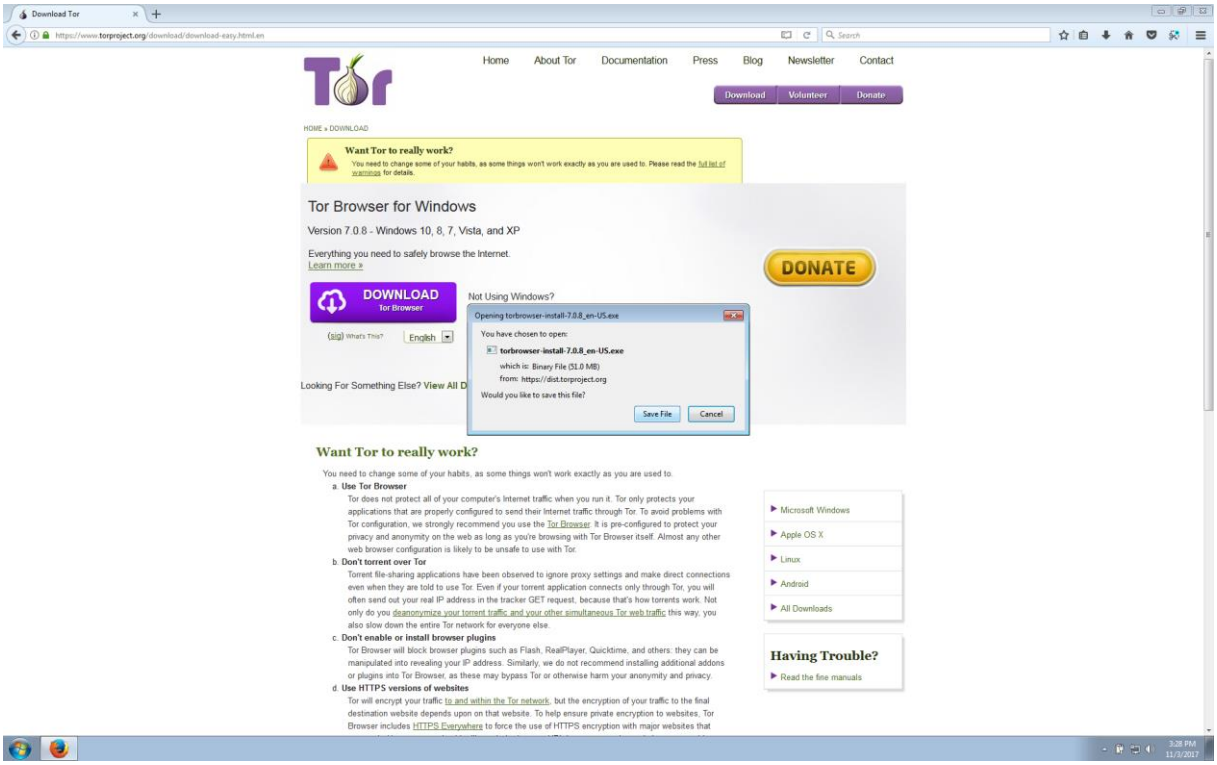
2.1 Instalacija

Tor Browser moguće je instalirati na računala s operacijskim sustavima Microsoft Windows na sljedeći način:

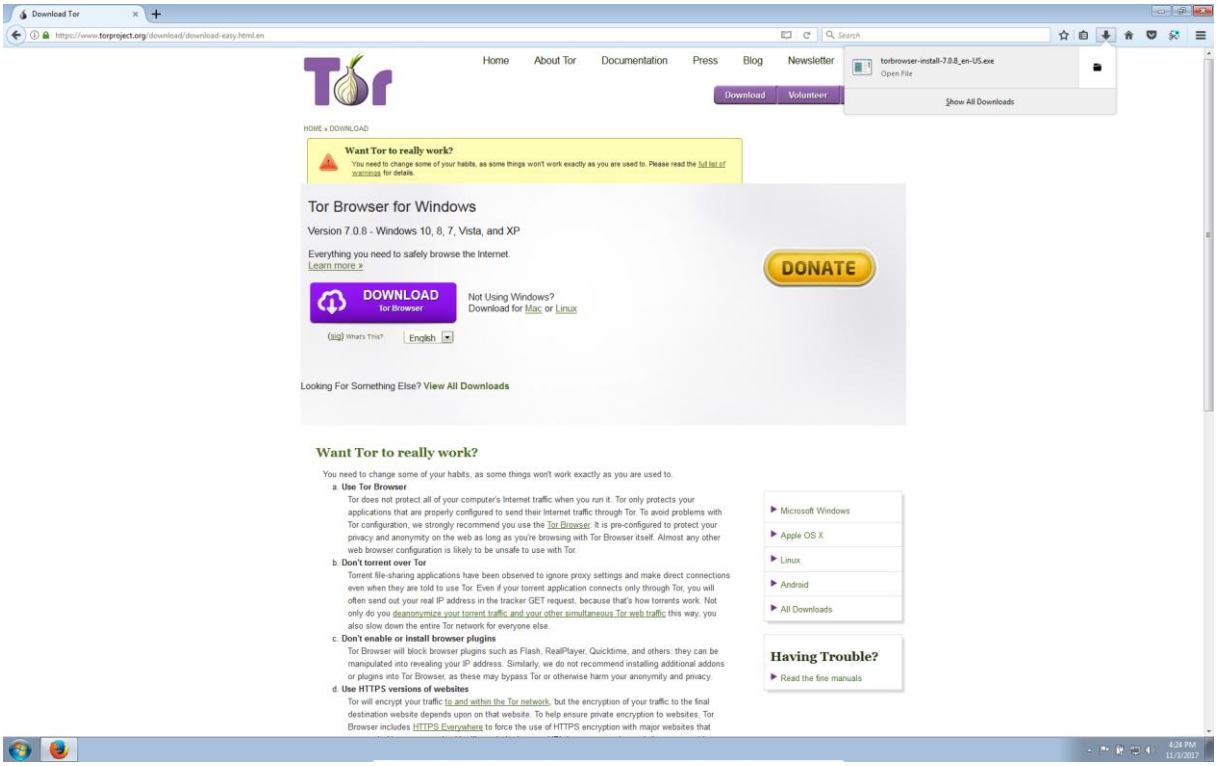
1. Prvo je potrebno preuzeti Tor Browser s ove poveznice klikom na ljubičastu ***Download*** tipku.



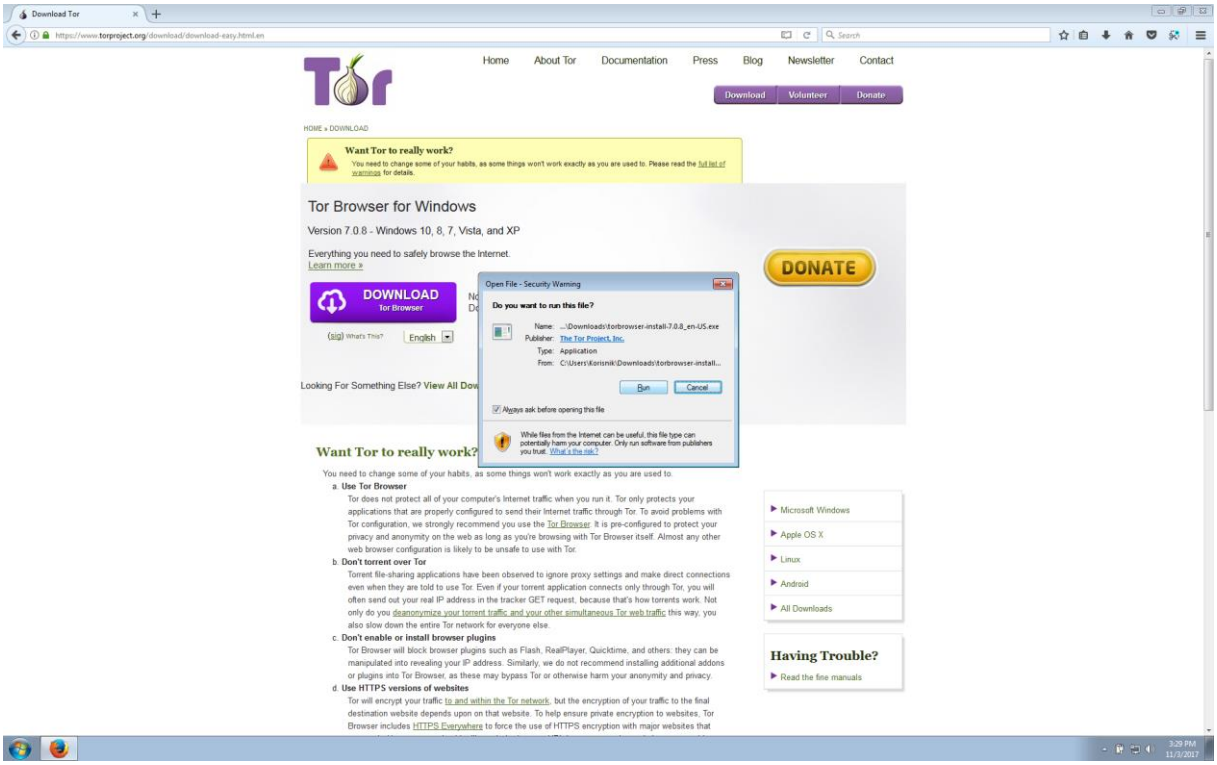
2. Zatim je potrebno kliknuti na *Save file* (ili ekvivalent u drugom Web pregledniku).



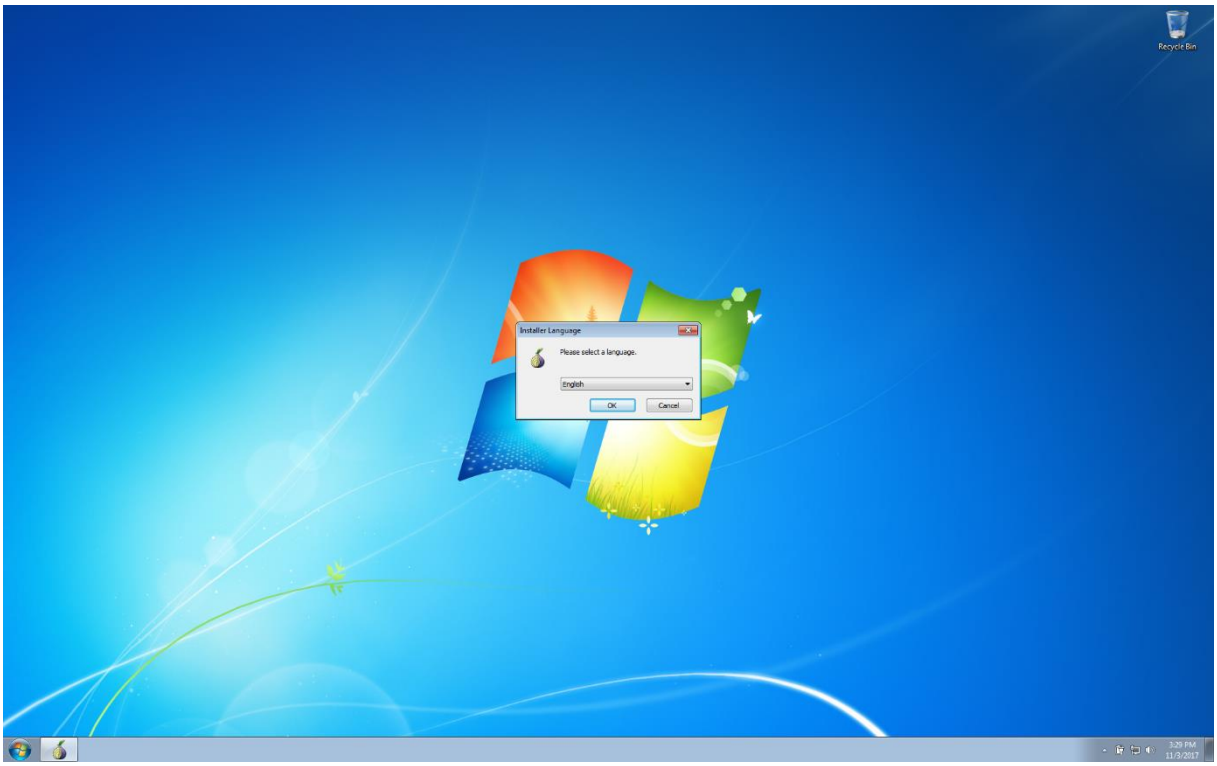
3. I konačno kada je preuzimanje gotovo, potrebno je pokrenuti preuzetu datoteku klikom unutar Web preglednika ili dvostrukim klikom izvan.



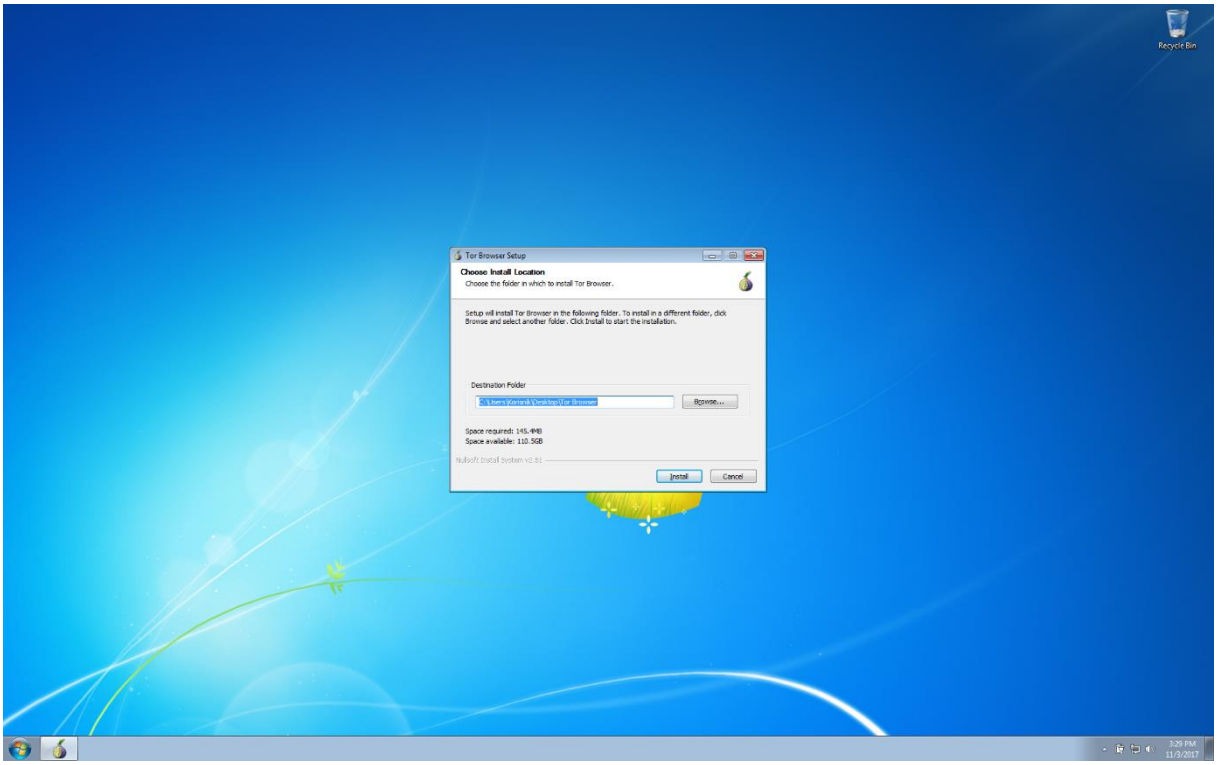
4. Zatim, ako se pojavi sljedeće upozorenje, kliknuti na ***Run***.



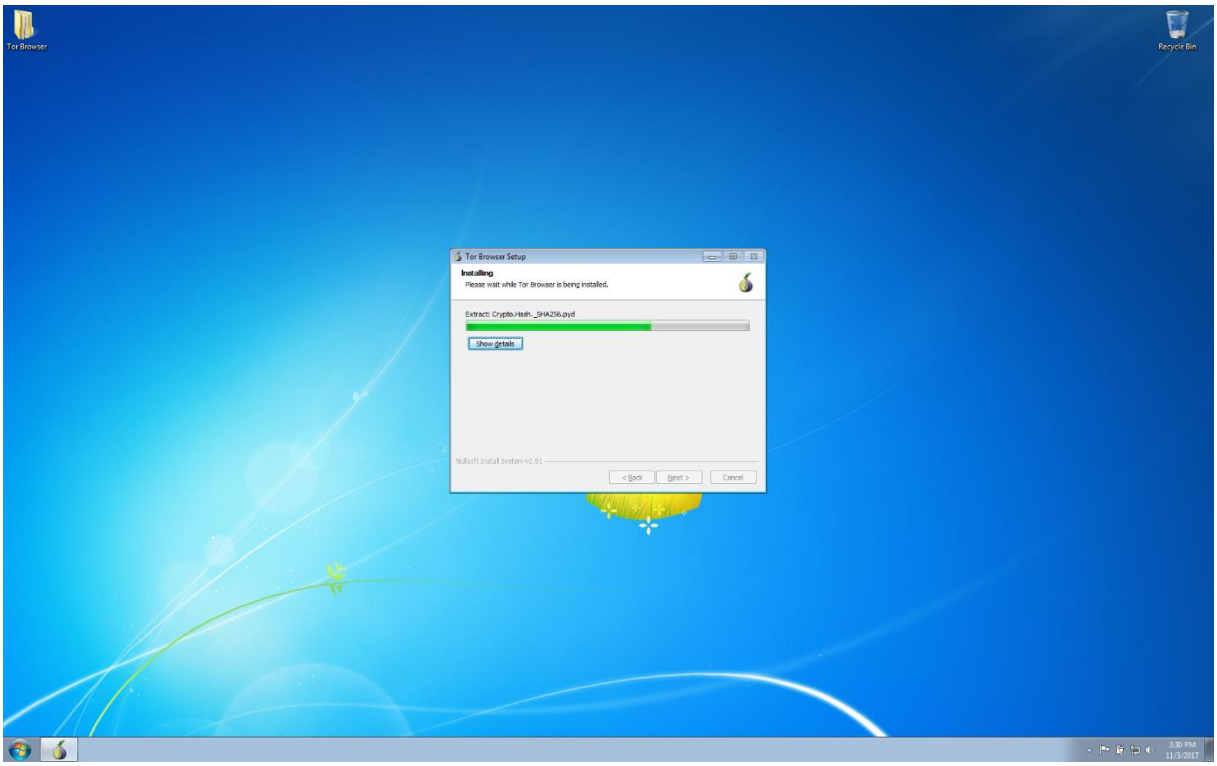
5. Kod pokretanja, prvo je potrebno odabrati jezik. Trenutno ne postoji hrvatski prijevod Tor Browser-a, tako da su daljnje upute pisane za Tor Browser na engleskom jeziku. Za nastavak instalacije, treba kliknuti na ***OK***.



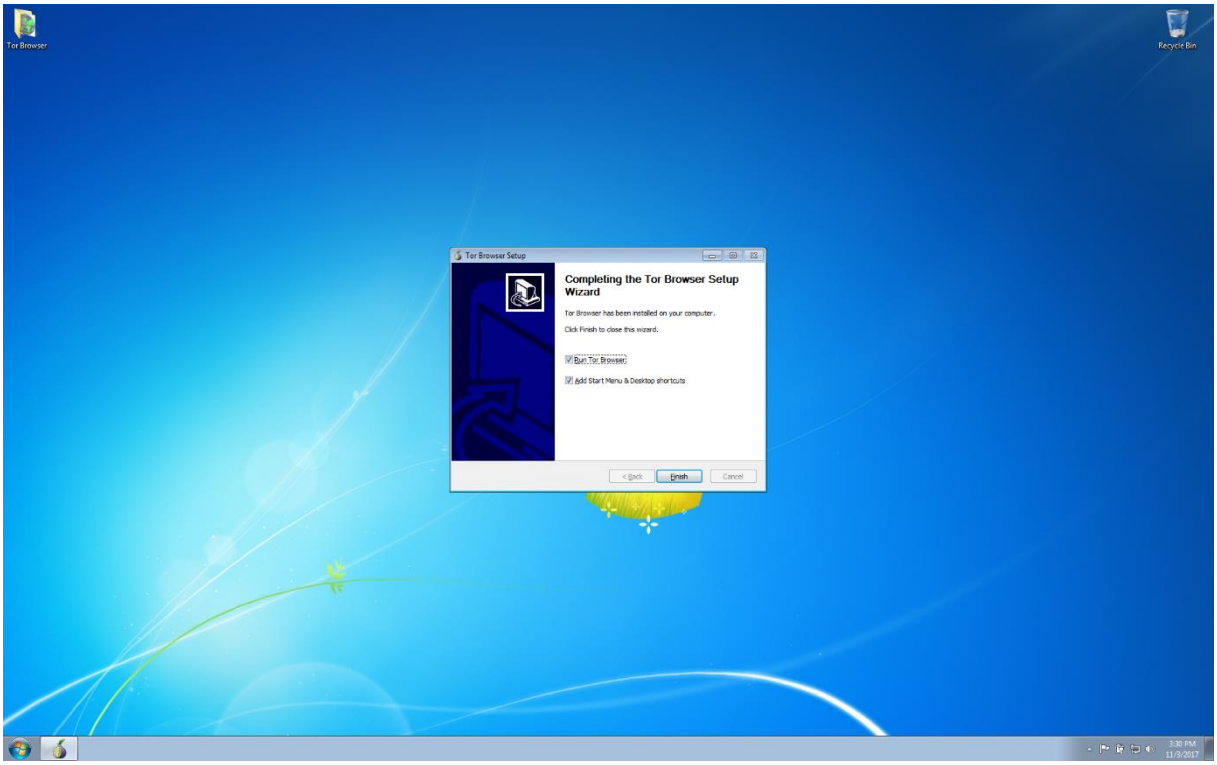
6. Zatim kliknuti na ***Next*** kako bi Tor Browser bio instaliran na radnu površinu (eng. *dekstop*).



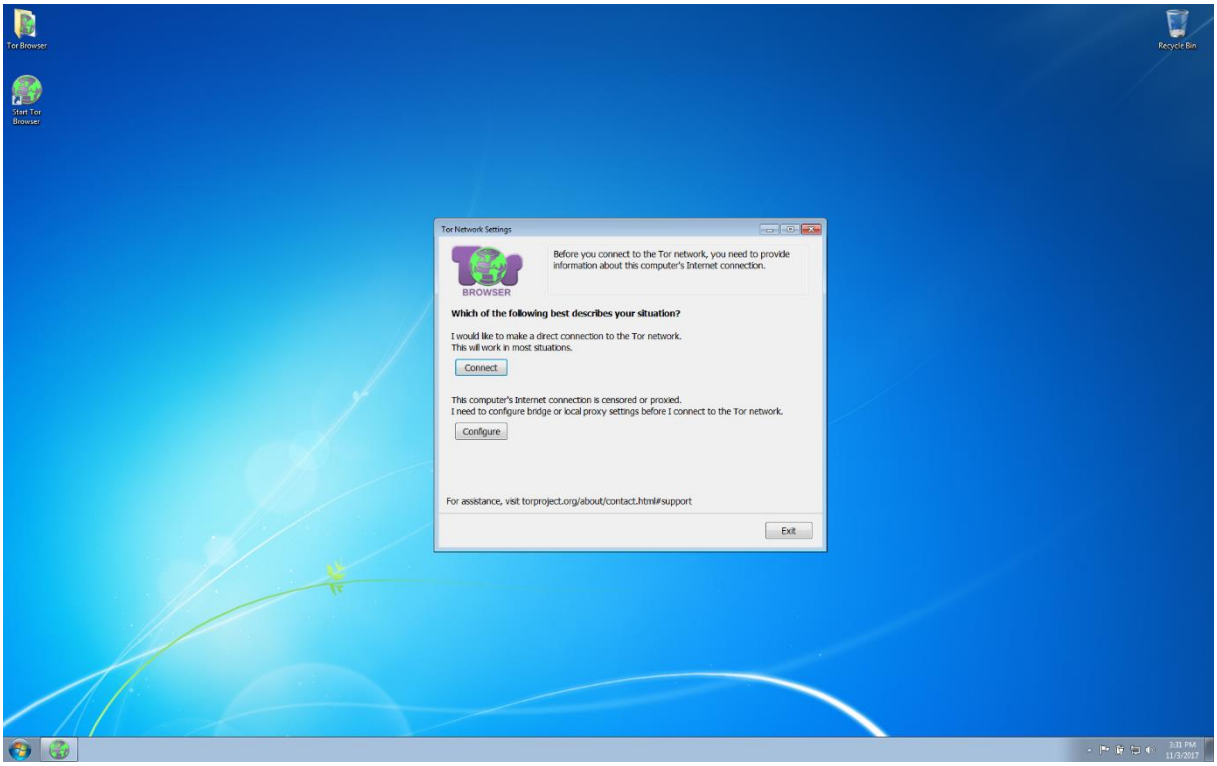
7. Potrebno je pričekati da postupak kopiranja datoteka završi te kliknuti na ***Next***.



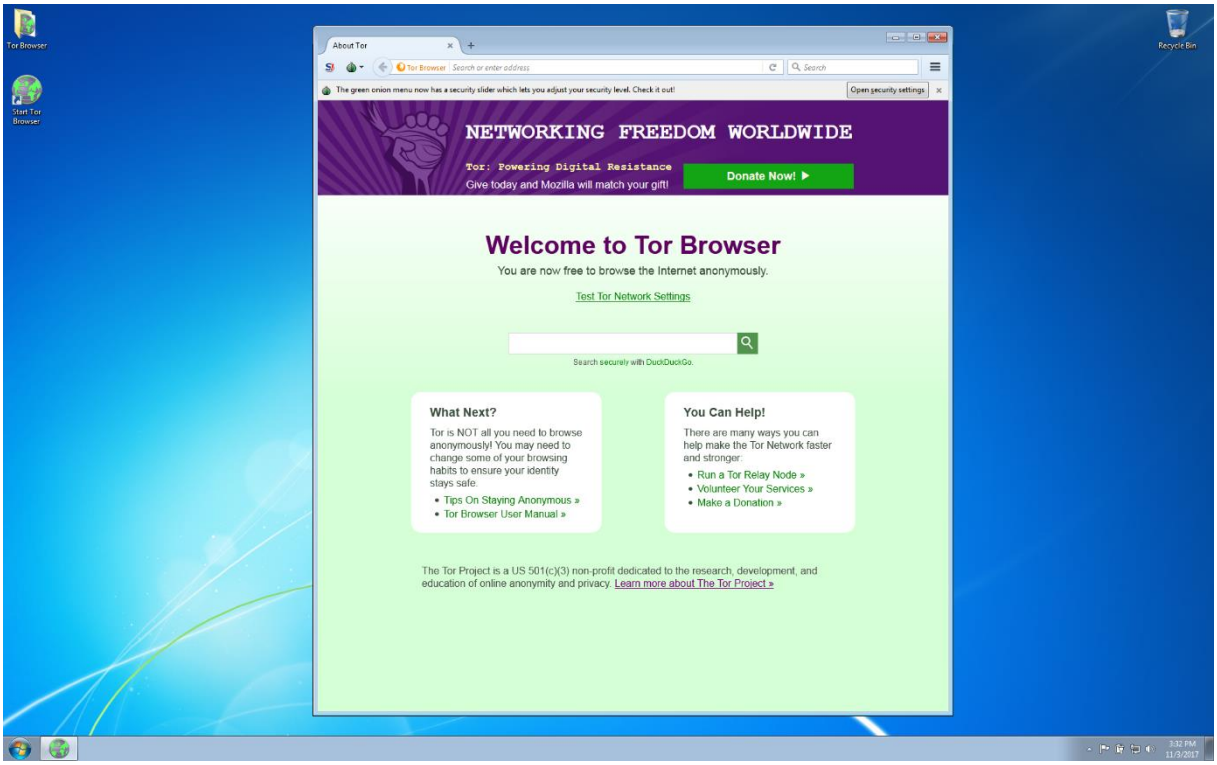
8. I konačno, treba kliknuti na ***Finish*** – nakon toga će se upaliti Tor Browser.



9. Kod prvog pokretanja pojavit će se sljedeći prozor – potrebno je kliknuti na ***Connect***. Dodatne korake umjesto klika na *Connect* moraju izvršiti samo korisnici koji su spojeni na mreže koje blokiraju pristup Tor mreži (takve probleme korisnici Interneta u Hrvatskoj u pravilu nemaju).



10. Nakon malo čekanja, trebao bi se pojaviti sljedeći prozor koji signalizira da je spajanje na Tor mrežu uspješno. U ovom je trenutku Tor Browser spreman za korištenje.



Prije korištenja Tor Browser-a pročitajte sljedeće poglavlje kako bi osigurali svoju anonimnost i privatnost.

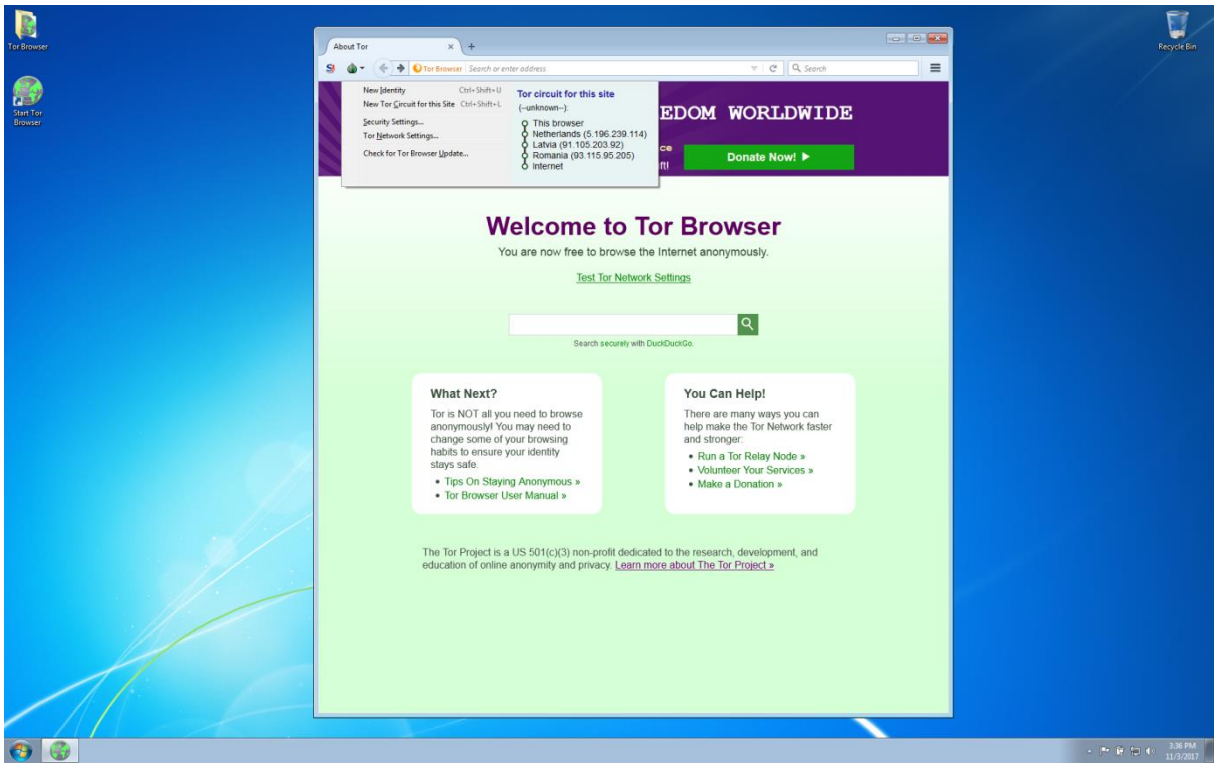
2.2 Kako sigurno koristiti Tor?

Tor je moćan sigurnosni alat s kojim je moguće anonimno i privatno koristiti Internet, **ali samo uz pridržavanje određenih pravila**.

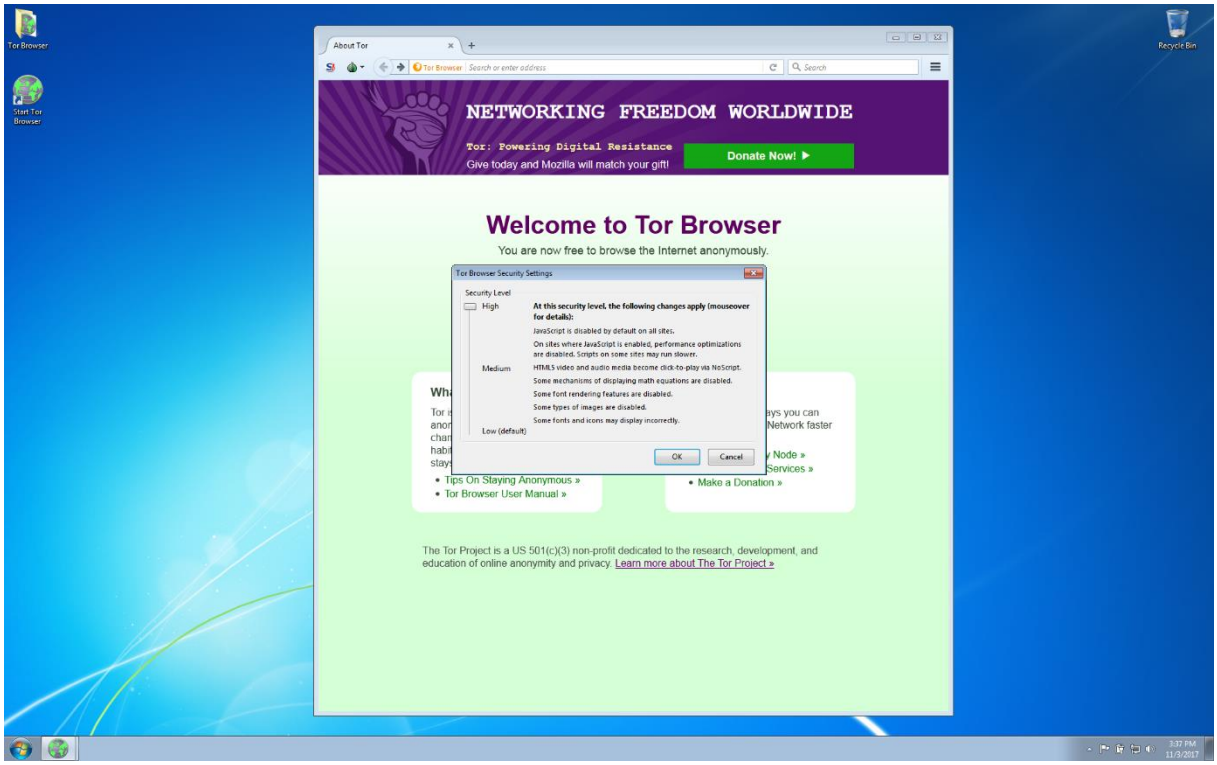
- Kao što je navedeno u uvodu, **zadnji korak** koji mrežne poruke prolaze – prijenos između trećeg volonterskog računala i odredišta – **nije zaštićen** sam po sebi. Kako bi korisnik ostao siguran, **nužno** je koristiti isključivo sigurne protokole, kao što je HTTPS, umjesto nesigurnih, kao što je HTTP.
    - Tor Browser dolazi s dodatkom (eng. *add-on*) *HTTPS everywhere* koji osigurava da korisnik koristi HTTPS prilikom posjećivanja velikog broja Web stranica, ali to **ne pokriva** sve stranice, između ostalog i zato jer neke stranice jednostavno nemaju HTTPS verziju i nije ih moguće sigurno koristiti (neovisno o Tor-u).
- Iako Tor štiti mrežni promet i informacije o njegovom izvoru odnosno odredištu – na mreži je moguće **vidjeti da se koristi Tor mreža**.
    - Primjerice, ako zaposlenik neke tvrtke koristi Tor mrežu, administrator sustava te tvrtke **može vidjeti da taj zaposlenik koristi Tor**. Administrator ne može znati sadržaj mrežnog prometa tog zaposlenika niti gdje je njegovo odredište, ali samo znanje da zaposlenik koristi Tor već može predstavljati problem. Ovo nije moguće zaobići u potpunosti, no aktivno se radi na tome da se to omogući korisnicima koliko god je moguće pomoću Tor mostova (eng. *Tor bridges*) i alata za maskiranje prometa (eng. *Tor pluggable transport*).
    - Isto vrijedi i na odredištu – primjerice, ako korisnik pristupa nekoj Web stranici pomoću Tor-a, ta Web stranica neće znati pravi identitet korisnika, ali **može znati da promet dolazi iz Tor mreže**. S obzirom da je to moguće znati, neki mrežni servisi blokiraju (ili otežavaju) pristup korisnicima iz Tor mreže jer smatraju da postoji povećani rizik od napada ako promet dolazi iz Tor-a.
- Korištenje Tor-a **ne znači** da je korisnik automatski potpuno anoniman – korisnik mora razumjeti na koji način koristi Internet i Web i otkriva li to na neki način njegov identitet.
    - Primjerice, ako korisnik pod imenom *Ivan Horvat* koristi Tor Browser, kroz njega se prijavi na *Facebook* u svoj korisnički račun i napiše neki komentar, svi će i dalje znati da je to napisao *Ivan Horvat* – Tor to nikako ne može spriječiti. Čak i bez ovakvih velikih grešaka ponekad je moguće povezati više informacija i otkriti koji je korisnik što napravio, unatoč korištenju Tor-a.
- Izrazito je bitno **ne otvarati nikakve datoteke** preuzete preko Tor Browser-a – ili barem to ne raditi dok je korisnikovo računalo spojeno na Internet. Velik broj različitih datoteka (npr. DOC i PDF dokumenti) ima mogućnost dohvata udaljenog mrežnog sadržaja – to je promet koji neće putovati kroz Tor, i kao posljedica može otkriti identitet krajnjeg korisnika.
- Tor i Tor Browser moćni su alati, ali **nisu neprobojni**. I uz savršeno korištenje Tor-a i Tor Browser-a, postoji mogućnost ugroza sigurnosti, anonimnosti i privatnosti **zbog**

još neotkrivenih propusta u Tor-u ili Tor Browser-u. Ako su posljedice ugroza sigurnosti, anonimnosti i privatnosti ozbiljne, nužno je imati više neovisnih slojeva zaštite (takozvani princip dubinske obrane – eng. *defense in depth*).

- Najbolje je Tor Browser što manje (idealno **nikako**) mijenjati – ne ugrađivati *Flash*, *Java*-u, *RealPlayer* i slično, ni ikakve dodatke (eng. *add-on*), idealno **čak i ne mijenjati veličinu prozora** (tj. ostaviti ga iste veličine kakav je kod pokretanja jer Web stranice mogu provjeravati veličinu korisnikovog prozora).
    - Svaka razlika od standardnog Tor browsera dodatni je rizik za anonimnost – najčešće zbog toga što se time korisnikov promet počinje razlikovati od prometa drugih Tor korisnika, što može olakšati deanonimizaciju.
- Postoji iznimka za prošlo pravilo – jedini način na koji je preporučljivo mijenjati Tor Browser je pomicanje sigurnosnog klizača na najsigurnije. To će isključiti pojedine mogućnosti preglednika (kao što je prikaz slika ili izvršavanje JavaScript koda) – ponekad i do te mjere da neke Web stranice neće uopće funkcionirati. No, u drugu ruku, to će znatno otežati napade i identifikaciju krajnjeg korisnika. To je moguće napraviti na sljedeći način – prvo kliknuti gore lijevo na zelenu sliku luka (Tor logo):



Pa zatim, klik na *Security settings* i pomicanje sigurnosnog klizača prema gore.



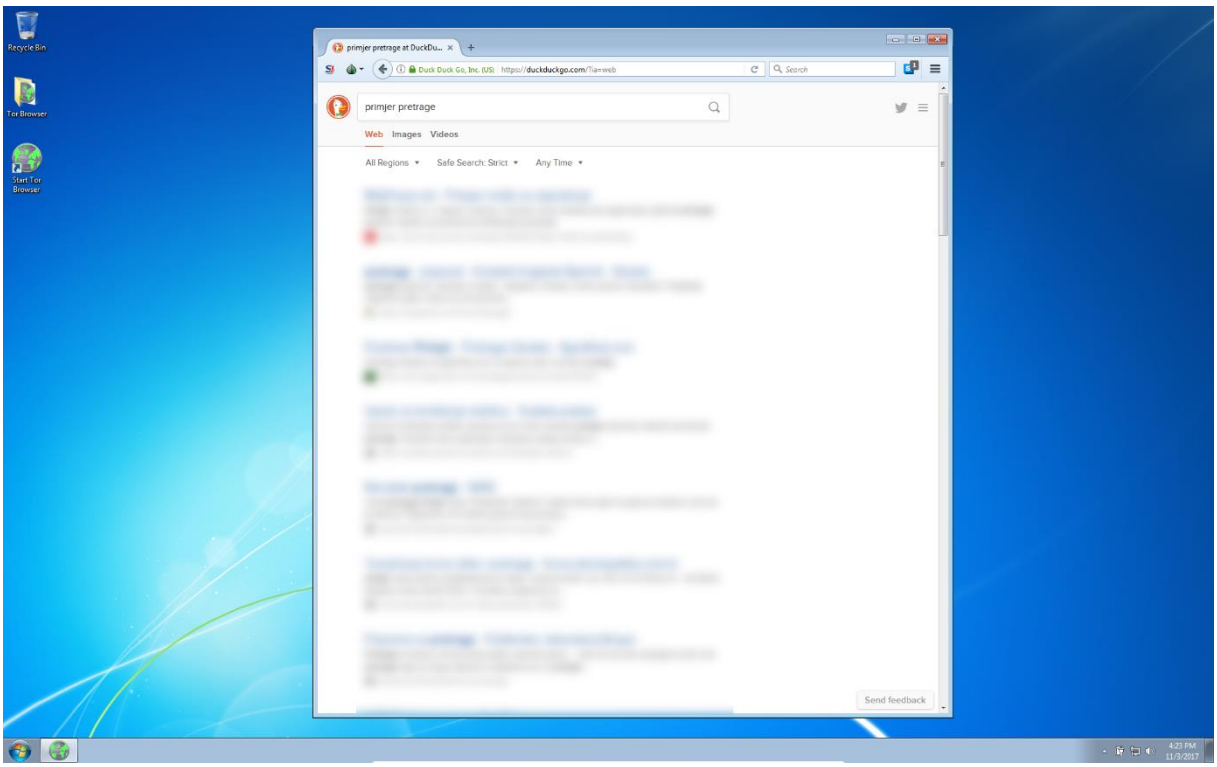
U konačnici, **nije moguće** ovim savjetima pokriti apsolutno sve slučajeve korištenja i potencijalnog ugrožavanja sigurnosti, anonimnosti i privatnosti. Ako postoje ozbiljne posljedice kod otkrivanja identiteta i narušavanja sigurnosti, nužno je **dobro se upoznati s potencijalnim rizicima i razumjeti ih** prije bilo kakvih radnja.

2.3 Korištenje

Tor Browser moguće je koristiti kao i svaki drugi Web preglednik:

- Primjerice, upisivanjem adrese *https://www.carnet.hr/* u lokacijsku traku na vrhu preglednika moguće je otvoriti Web stranice CARNet-a. Na isti način moguće je otvoriti i druge stranice, primjerice tražilicu *Google* (https://www.google.hr/).
    - Glavna razlika od drugih Web preglednika je **sporija veza zbog korištenja Tor mreže** – uobičajeno je da otvaranje Web stranice traje oko minute, umjesto nekoliko sekunda kada se ne koristi Tor mreža.
    - Kao što je navedeno u prethodnom poglavlju, neki mrežni servisi kao što su Web stranice blokiraju ili otežavaju pristup korisnicima koji koriste Tor mrežu, tako da postoji mogućnost da nekim Web stranicama nije moguće pristupiti pomoću Tor Browser-a ili da traže dodatne provjere prije korištenja.

- Upisivanjem pojmova u lokacijsku traku izvršit će se pretraga pomoću tražilice *DuckDuckGo* – to je Web tražilica slična drugim takvim tražilicama (kao što su *Google* i *Bing*) po funkcionalnost i načinu korištenja, samo sa većim fokusom na privatnost.

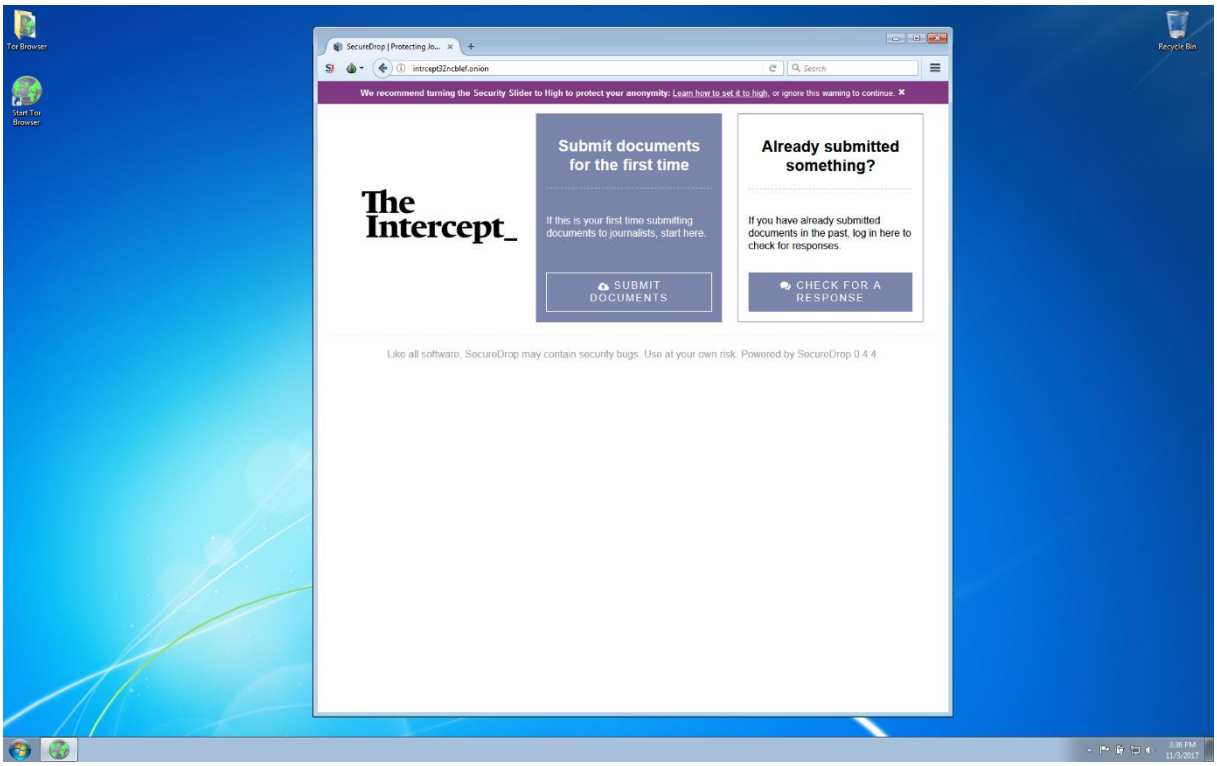


- U Tor Browser-u je moguće pristupati i tzv. Tor sakrivenim servisima (eng. *Tor hidden services*). To su posebni servisi koji su zbog privatnosti i anonimnosti (kako korisnika, tako i vlasnika servisa) dostupni samo kroz Tor mrežu.

    - Kod korištenja Tor sakrivenih servisa – mrežni promet nikad **ne izlazi iz Tor mreže**. To ima dvije posljedice: kao prvo, promet je u potpunosti šifriran od korisnika do servisa (eng. *end-to-end encrypted*), a kao drugo **korisnik ne zna tko je zapravo vlasnik servisa i vlasnik servisa ne zna tko su mu korisnici**. Na taj način osigurana je visoka razina anonimnosti i za korisnike i vlasnike/administratore servisa.

    - Tor sakrivene servise moguće je prepoznati po domeni koja završava s *.onion*. Primjerice, na adresi *http://intrcept32ncblef.onion/* moguće je pristupiti sakrivenom servisu novinske organizacije *The Intercept*, na kojem im je moguće na anoniman način dostaviti povjerljive informacije. To je primjerice korisno zviždačima (eng. *whistleblowers*) – korištenjem Tor sakrivenog servisa znaju da Tor osigurava da čak ni *The Intercept* ne zna tko im šalje podatke, a isto tako ni bilo tko drugi.

    - Mreža Tor sakrivenih servisa jedna je od tzv. tamnih mreža (eng. *darknet*), a Web stranice na takvim servisima dio su tamnog Web-a (eng. *dark web*) i često se krivo nazivaju dubokim Web-om (eng. *deep web*).



3 Zaključak

Tor Browser moćan je alat za **anonimno i privatno pregledavanje Web-a** i Tor sakrivenih servisa. Mrežni promet Tor Browser-a prolazi kroz Tor mrežu anonimnosti, gdje je tehnikom slojevitog usmjeravanja **sadržaj mrežnog prometa zaštićen**, a njegov **mrežni put prikriven**.

Tor Browser ima **velik broj raznolikih korisnika** i **dostupan je svima**. Za njegovo korištenje potrebno je samo računalo, veza na Internet i slobodno dostupni alati. Građani mogu koristiti Tor Browser kako bi anonimno i privatno pregledavali Web i zaobišli cenzure.

Ovaj dokument dao je uvod u svrhu i način rada Tor mreže (poglavlje 1) i upute za instalaciju (poglavlje 2.1) i korištenje (poglavlje 2.3) Tor Browser-a. Kako bi korisnici zaista ostali anonimni i privatno pregledavali Web pomoću Tor Browsera, potrebno je imati na umu određene koncepte i držati se nekih pravila koja su navedena u poglavlju 2.2. Nažalost, nije moguće pokriti sve slučajeve korištenja i potencijalnog ugrožavanja sigurnosti, anonimnosti i privatnosti tim pravilima, tako da ako postoje ozbiljne posljedice kod otkrivanja identiteta i narušavanja sigurnosti, nužno je **dobro se upoznati s potencijalnim rizicima i razumjeti ih** prije bilo kakvih radnja.

U konačnici, informacije i znanja sadržana u ovom dokumentu mogu biti korisni svim građanima, neovisno o tome jesu li trenutno zabrinuti za svoju anonimnost i privatnost svoje komunikacije. Znanja i vještine sigurnog, anonimnog i privatnog korištenja Interneta postaju sve korisnije u današnjem svijetu gdje se svakim danom sve više infrastrukture i svakodnevnih radnji oslanja upravo na Internet.