

Tor mreža - tehnička pozadina i napredno korištenje

NCERT-PUBDOC-2018-2-356

Sadržaj

1	UVOD	4
2	TEHNIČKA POZADINA TOR MREŽE	5
2.1	IMENICI TOR ČVOROVA (ENG. <i>DIRECTORY AUTHORITIES</i>)	6
2.2	ENTRY GUARD	6
2.3	TOR MOSNI ČVOROVI (ENG. <i>TOR BRIDGE RELAYS</i> ILI <i>BRIDGES</i>).....	7
2.4	UKLOPNI PRIJEVOZNICI (ENG. <i>PLUGGABLE TRANSPORTS</i>).....	8
2.5	TOR SAKRIVENI SERVISI (ENG. <i>TOR HIDDEN SERVICES</i> ILI <i>ONION SERVICES</i>)	8
3	NAPREDNO KORIŠTENJE TOR MREŽE	10
3.1	TAILS.....	10
3.1.1	<i>Instalacija Tailsa</i>	10
3.1.2	<i>Korištenje Tailsa</i>	11
3.2	WHONIX	13
3.2.1	<i>Instalacija</i>	13
3.2.2	<i>Korištenje</i>	14
3.3	KONFIGURACIJA VLASTITOG SAKRIVENOG SERVISA.....	16
4	ZAKLJUČAK	19
5	LITERATURA	20

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Tor je mreža anonimnosti koja korisnicima omogućuje visoku razinu privatnosti i anonimnosti pri korištenju Interneta. Tor mreža sastoji se od brojnih volonterskih računala kroz koje prolazi kriptografski zaštićen promet korisnika mreže.

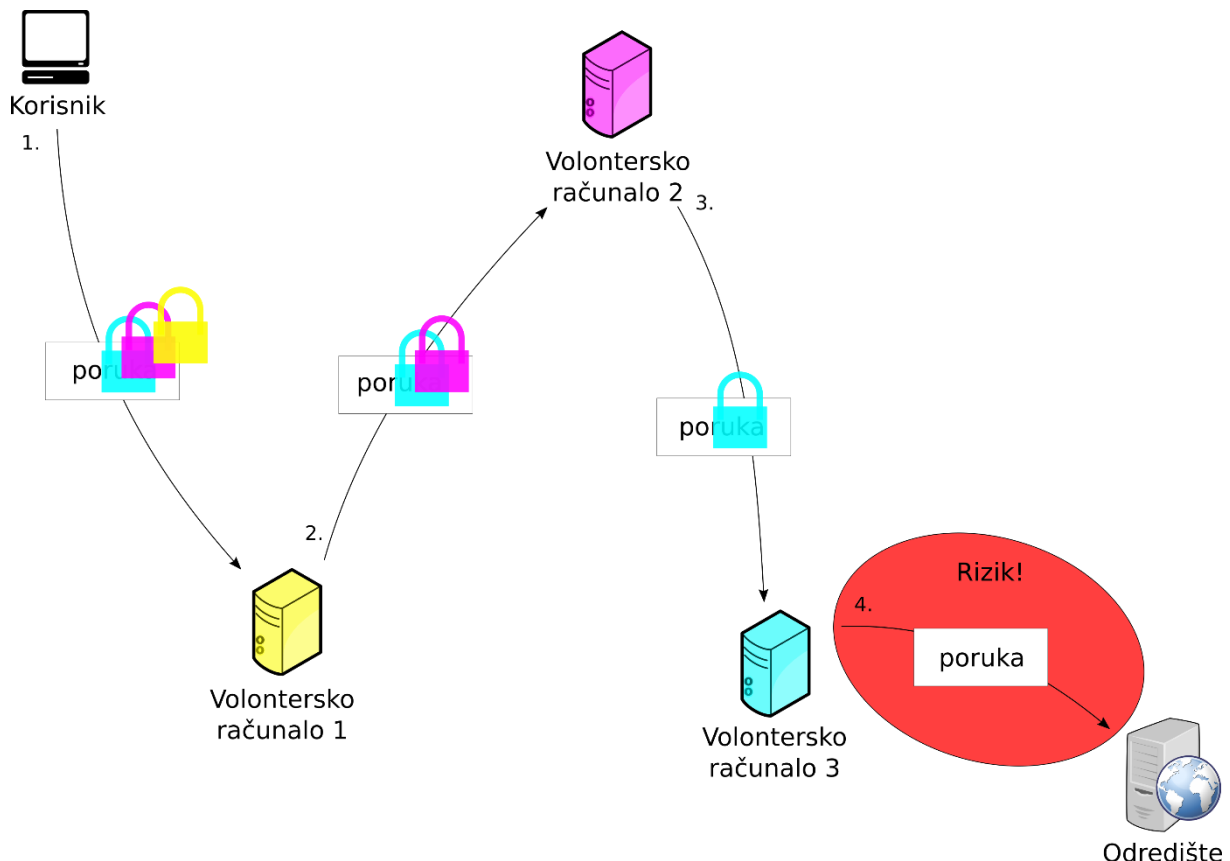
Ovaj dokument namijenjen je osobama koje imaju osnovno znanje korištenja Tor mreže i Tor Browsera (Tor Web preglednika). Osnovno objašnjenje Tor mreže te upute za instalaciju i korištenje Tor Browsera nalaze se u [prethodno objavljenom dokumentu](#) Nacionalnog CERT-a.

U ovom dokumentu objašnjena je tehnička pozadina Tor mreže te neki od naprednih koncepata na kojima se temelje sigurnosne pretpostavke Tora. Također, Tor služi kao temeljna tehnologija na kojoj su izgrađeni drugi, specijalizirani alati, od kojih će par poznatijih biti opisano u ovom dokumentu.

2 Tehnička pozadina Tor mreže

Sam naziv „Tor“ izvorno je nastao kao skraćenica od engleskog naziva *The Onion Router*. Taj naziv moguće je prevesti kao „slojeviti usmjerivač“, zbog slojevitog načina rada Tor mreže. Promet Tor mreže prvo je trostruko šifriran te zatim prolazi kroz tri nasumično odabrana Tor čvora gdje se na svakom čvoru dešifrira jedan sloj. Treći čvor dešifrira zadnji sloj te korisnikovu poruku šalje na odredište.

Općenito, ovakvim šifriranjem i usmjeravanjem prometa, Tor prikriva tragove te otežava analizu korisnikovog prometa. Dijagram na slici 1 prikazuje kako promet korisnika putuje kroz Tor mrežu do njegovog odredišta te kako se taj promet putem slojevito dešifrira.



Slika 1 – Put i slojevito dešifriranje korisnikovog prometa kroz Tor mrežu

Važno je biti svjestan kako Tor ne može šifrirati promet između zadnjeg čvora i odredišta – taj dio odgovornost je korisnika. U većini slučajeva, iz perspektive korisnika to se može riješiti korištenjem HTTPS umjesto HTTP protokola.

Glavni dio Tora kao mreže su Tor čvorovi (eng. *Tor nodes, relays* ili *routers*). Tor čvor je zapravo bilo koje računalo na kojem radi Tor softver kao prenositelj poruka (eng. *relay*) umjesto kao korisnik mreže. Tor čvorove postavljaju i održavaju volonteri diljem svijeta te ih trenutno ima preko 8.000. No nisu svi Tor čvorovi isti – različite uloge imaju, primjerice, zaštitnici ulaza (eng. *entry guards*) i mosni čvorovi (eng. *bridge relays*). Također, Tor čvorovi nisu jedini dio mreže – Tor mreža ne bi mogla funkcionirati bez imenika Tor čvorova (eng. *directory authorities*). Ovi i još neki koncepti bit će objašnjeni u nastavku ovog poglavlja.

2.1 Imenici Tor čvorova (eng. *directory authorities*)

Kako bi se korisnik mogao spojiti na Tor mrežu, Tor (kao softver na računalu korisnika) prvo treba **saznati koji čvorovi postoje**. Kako bi to bilo moguće napraviti na siguran način, u Tor softver ugrađene su IP adrese i kriptografski ključevi tzv. **imenika Tor čvorova** (eng. *directory authorities*). Kako bi saznao koji čvorovi postoje, Tor softver na korisničkom računalu radi sljedeće:

1. **Preuzima popis** Tor čvorova od bilo kojeg imenika Tor čvorova. Taj popis bi u pravilu trebali digitalno potpisati **svi** imenici Tor čvorova.
2. Pomoću ugrađenih kriptografskih ključeva **provjerava koliko** imenika Tor čvorova je **zaista** ispravno potpisalo preuzeti popis.
3. Ako je popis ispravno potpisala **većina** (više od pola) **imenika Tor čvorova**, on se smatra valjanim te se koristi za spajanje na Tor mrežu.

Ovaj proces osigurava da, ako napadač želi kompromitirati popis Tor čvorova, on mora uspješno kompromitirati više od pola imenika Tor čvorova.

Trenutno postoji devet imenika Tor čvorova te još jedan posebni imenik za mosne čvorove koji će biti objašnjeni kasnije. Imenike Tor čvorova pokreću i održavaju osobe koje su već dugo aktivne u Tor zajednici te kojima Tor zajednica općenito vjeruje. Trenutni popis imenika Tor čvorova te još neke njihove detalje moguće je vidjeti [ovdje](#).

Kako bi se imenici Tor čvorova mogli dogovoriti te potpisati jedan popis Tor čvorova, oni svakih sat vremena glasaju te postižu konsenzus oko trenutnog stanja Tor mreže. Rezultat konsenzusa je popis Tor čvorova koji zatim u pravilu potpisuju svi imenici Tor čvorova. U konačnici, taj digitalno potpisani popis Tor čvorova preuzimaju i koriste korisnici Tor mreže, kao što je prethodno objašnjeno.

2.2 Zaštitnici ulaza (eng. *entry guards ili guard nodes*)

Jedna od glavnih mana Tor mreže je to što ona ne može osigurati anonimnost korisnika ako napadač nadzire oba kraja njegove komunikacije. Jednostavnijim rječnikom, problem nastaje kada napadač može vidjeti:

1. Promet korisnika dok ulazi u Tor mrežu – to primjerice može vidjeti korisnikov pružatelj mrežnih usluga ili prvi (ulazni) Tor čvor kojeg korisnik koristi.
2. Promet korisnika kako izlazi iz Tor mreže – to primjerice može vidjeti Web stranica koju korisnik posjećuje, njen pružatelj mrežnih usluga ili treći (izlazni) Tor čvor kojeg korisnik koristi.

Konkretni scenarij napada može izgledati ovako – napadač ima kontrolu nad prvim (ulaznim) Tor čvorom kojeg žrtva koristi i nad Web stranicom koju ona posjećuje. Tada, napadač na ulazu u Tor mrežu i dalje ne vidi što žrtva šalje preko Tor mreže jer je promet šifriran. Na drugom kraju, napadač vidi da Web stranica ima brojne posjetitelje, no ne zna je li jedan od njih i žrtva, te ako je, što ona radi na Web stranici.

No analizom prometa, tj. uspoređivanjem vremena i veličine paketa koje žrtva šalje u Tor mrežu te paketa koji stižu na Web stranicu, napadač može s visokom pouzdanošću potvrditi da žrtva posjećuje Web stranicu i otkriti što točno ona radi na njoj. Na taj način, unatoč tome što žrtva koristi Tor mrežu, njena anonimnost je kompromitirana.

Trenutno, glavni mehanizmi sprječavanja takvih napada u Tor mreži svode se na to da otežaju napadaču mogućnost da nadzire oba kraja komunikacije korisnika kojeg pokušava deanonimizirati.

Kao što je objašnjeno u primjeru, nije poželjno da napadač ima kontrolu nad prvim (ulaznim) Tor čvorom nekog korisnika. Kako bi se smanjila ta mogućnost, uveden je koncept tzv. **zaštitnika ulaza** (eng. *entry guards*). Tor softver će prilikom spajanja na Tor mrežu za ulazne čvorove birati samo čvorove sa **zastavicom zaštitnika** (eng. *guard flag*). To je zastavica koju imenici Tor čvorova dodjeljuju čvorovima koji su već duže vrijeme dio mreže te koji obrađuju veću količinu prometa. Na taj način, napadači ne mogu, s malo resursa, postaviti veliki broj Tor čvorova i time povećati mogućnost da ih meta odabere za ulazni čvor.

Također, kada bi korisnik redovito mijenjao prvi (ulazni) Tor čvor, bilo bi samo pitanje vremena kada bi odabrao napadačev čvor te time mu potencijalno omogućio napad. Zbog toga, jednom kada korisnikov Tor softver odabere ulazni čvor, neće ga mijenjati neko duže vrijeme. Na ovaj način, povećava se vjerojatnost da napadač nikada neće kontrolirati ulazni čvor, dok se najgori slučaj, u kojem napadač kontrolira ulazni čvor, ne mijenja značajno.

2.3 Tor mosni čvorovi (eng. *Tor bridge relays* ili *bridges*)

Zbog raznih razloga, pružatelji mrežnih usluga, institucije nekih država i drugi ponekada **blokiraju** pristup Tor mreži. Kao što je prethodno objašnjeno, od imenika Tor čvorova moguće je preuzeti popis Tor čvorova, uključujući i njihove IP adrese. Pomoću tog popisa, cenzori mogu lako zabraniti pristup Tor mreži **blokiranjem veza s IP adresama Tor čvorova**.

Kako bi se zaobišlo takvo blokiranje Tor mreže, uveden je koncept **Tor mosnih čvorova** (eng. *Tor bridge relays* ili *Tor bridges*). Mosni čvorovi slični su običnim Tor čvorovima, no njihove IP adrese se **ne nalaze u javnim imenicima** Tor čvorova niti postoji neki drugi javni i potpuni popis mosnih čvorova. Zbog toga, cenzori nemaju jednostavan način za blokiranje pristupa svim mosnim čvorovima. Korisnici kojima cenzori blokiraju pristup uobičajenim Tor čvorovima mogu se u pravilu na Tor mrežu spojiti **preko mosnih čvorova**.

Glavni problem u izvedbi cijelog koncepta mosnih čvorova je sljedeći – kako osigurati da legitimni korisnici mogu doći do informacija o mosnim čvorovima, no istovremeno spriječiti da to mogu cenzori? Taj problem nažalost nije moguće u potpunosti riješiti. Trenutno, do informacija o nekoliko mosnih čvorova moguće je doći na sljedeće načine:

1. Posjetom Web stranice na adresi <https://bridges.torproject.org/>
2. Slanjem poruke elektroničke pošte na adresu *bridges@torproject.org* s linijom „*get bridges*“ u tijelu poruke.

3. Preuzimanjem Tor Browsera s kojim automatski dolaze i informacije o par mosnih čvorova.

Kako bi se smanjila mogućnost da cenzori automatski sastave popis mosnih čvorova pomoću ovih mehanizama, uvedena su određena ograničenja. Primjerice, na Web stranici za dohvat informacija o mosnim čvorovima potrebno je ispuniti *CAPTCHA* izazov, dok je za dohvat putem elektroničke pošte potrebno poslati zahtjev s usluga elektroničke pošte *Gmail*, *Yahoo* ili *Riseup*.

Upute za konfiguraciju korištenja mosnih čvorova u Tor Browseru te više informacija o mosnim čvorovima dostupno je [ovdje](#).

2.4 Uklopni prijevoznici (eng. *pluggable transports*)

Blokiranje IP adresa Tor čvorova nije jedina tehnika kojom cenzori blokiraju pristup Tor mreži. Napredni cenzori analiziraju mrežni promet korisnika te i na taj način pokušavaju otkriti koriste li oni Tor mrežu.

Primjerice, korisnik koristi mosni čvor za pristup Tor mreži te cenzor ne zna da je to zapravo Tor čvor. No analizom mrežnog prometa između korisnika i mosnog čvora, cenzor može prepoznati da se radi o spajanju na Tor mrežu te blokirati tu vezu.

Kako bi se zaobišao ovaj način blokiranja Tor mreže, stvoreni su tzv. **uklopni prijevoznici** (eng. *pluggable transports*). Uklopni prijevoznici su mehanizmi maskiranja prometa između korisnika i mosnog čvora Tor mreže kako bi se sakrila činjenica da se zapravo radi o prometu Tor mreže.

Upute za konfiguraciju korištenja uklopnih prijevoznika u Tor Browseru te više informacija o uklopnim prijevoznicima dostupno je [ovdje](#).

2.5 Tor sakriveni servisi (eng. *Tor hidden services* ili *onion services*)

Uobičajeno korištenje Tor mreže omogućava korisnicima anonimnost prilikom komunikacije s poslužiteljima kako bi npr. pregledavali Web stranice ili komunicirali pomoću *instant messaging/chat* aplikacija. No i neki pružatelji usluga imaju potrebu za anonimnošću, tj. za osiguravanjem anonimnosti svojih mrežnih poslužitelja. Česti primjer toga su novinarske Web stranice i blogovi koji žele izbjeći progon i cenzuru u totalitarnim režimima zbog informacija koje objavljuju. Tor im to omogućava putem **Tor sakrivenih servisa** (eng. *Tor hidden services* ili *onion services*).

Tehnička pozadina Tor sakrivenih servisa prilično je složena. Uz to, trenutno se uvodi i nova inačica sustava zvana „Tor sakriveni servisi nove generacije“ (eng. *next-generation Tor onion services*). U suštini, Tor sakriveni servisi su poslužitelji koji se nalaze „unutar“ Tor mreže. To kao posljedicu ima sljedeće:

1. Umjesto prave domene na Internetu (npr. *carnet.hr*), sakriveni servisi imaju **posebnu .onion domenu** oblika *<16 alfanumeričkih znakova>.onion*, primjerice *nytimes3xbfgragh.onion*.

2. Skrivenim servisima moguće je pristupiti **isključivo** kroz Tor mrežu. Primjerice, ako korisnik u svoj Web preglednik koji ne koristi Tor mrežu upiše *nytimes3xbfgragh.onion*, javit će se greška. To je Web stranica na Tor sakrivenom servisu i njoj se može pristupiti isključivo kroz Tor mrežu, primjerice kroz Tor Browser. Upravo zbog ovoga, sakriveni servisi općenito su dio tzv. **tamne mreže** (eng. *darknet*), a Web stranice na sakrivenim servisima su dio tzv. **tamnog Weba** (eng. *dark web*).
3. S tehničke strane, mrežni promet između korisnika i Tor sakrivenog servisa putuje kroz **šest Tor čvorova**, za razliku od uobičajena tri Tor čvora između korisnika Tor mreže i odredišta na Internetu. Tri Tor čvora bira korisnik, a tri bira sakriveni servis što u konačnici osigurava i anonimnost korisnika i sakrivenog servisa. Drugim riječima, **korisnik ne zna identitet sakrivenog servisa, niti sakriveni servis zna identitet korisnika**. No kao posljedica ovakvog dužeg puta kroz Tor mrežu, veza između korisnika i sakrivenog servisa obično je prilično spora.

Više o trenutnoj inačici Tor sakrivenih servisa moguće je pročitati [ovdje](#), dok je više o nadolazećoj inačici, Tor sakrivenim servisima nove generacije, moguće pročitati [ovdje](#).

3 Napredno korištenje Tor mreže

Kako bi se omogućilo jednostavnije, a sigurno korištenje Tor mreže te kako bi se uveli dodatni slojevi sigurnosti, razvijeni su razni alati koji koriste Tor kao temelj svog rada. Primjeri takvih alata su operacijski sustavi Tails i Whonix koji će biti opisani u ovom poglavlju.

Također, Tor mrežu moguće je koristiti i za anonimno pružanje mrežnih usluga. U ovom poglavlju će ukratko biti opisano kako to učiniti postavljanjem Tor sakrivenih servisa.

3.1 Tails

Tails (skraćeno od eng. *the amnesic incognito live system*) je operacijski sustav namijenjen očuvanju privatnosti i anonimnosti. Za razliku od konvencionalnih operacijskih sustava, Tails se obično instalira na USB *stick* ili na DVD te se preko njih pokreće. Zbog toga je Tails moguće koristiti s gotovo bilo kojeg računala (ne samo na vlastitim računalima, već primjerice i u knjižnici) te on tijekom rada na računalu neće ostaviti nikakve tragove.

Tails, kao i alati koji dolaze s njim, slobodan je softver (eng. *free and open source software*). Tails dolazi s brojnim alatima za svakodnevnu uporabu, kao što su Web preglednik, uredski programi, klijent za e-poštu, alat za uređivanje slika itd. Za anonimnu i privatnu komunikaciju Tails se oslanja na Tor mrežu, te je konfiguriran na sljedeći način:

- Svi programi konfigurirani su da koriste Tor mrežu.
- Ako se neki program pokuša povezati na Internet izravno umjesto preko Tor mreže, Tails će tu vezu blokirati.

Kako se Tails u pravilu pokreće s USB *stick* ili DVD-a, njegovo korištenje se ne mijenja i ne ovisi o operacijskom sustavu koji je instaliran na računalo, tj. na tvrdi disk računala.

Kao i kod drugih alata za sigurnost i privatnost, važno je razumjeti ograničenja operacijskog sustava Tails i alata koji dolaze s njim. Više informacija o rizicima prilikom korištenja Tailsa dostupno je [ovdje](#).

3.1.1 Instalacija Tailsa

Detaljne upute za instalaciju Tailsa s operacijskih sustava Windows, macOS i Linux dostupne su [ovdje](#).

Kako bi se omogućila sigurna konfiguracija automatskih nadogradnji te šifrirana trajna memorija na USB *sticku*, potrebno je Tails instalirati preko programa *Tails Installer*. *Tails Installer* dostupan je na postojećoj instalaciji Tailsa ili na novijim inačicama Linux distribucija Debian, Ubuntu i Mint. Za instalaciju s ostalih operacijskih sustava, kao npr. Microsoft Windows, potrebna su 2 USB *stick*a. Jedan služi kao posredni USB *stick* na koji se instalira Tails bez navedenih značajki, ali s kojeg se može instalirati potpuni Tails sa svim značajkama pomoću *Tails Installer* programa.

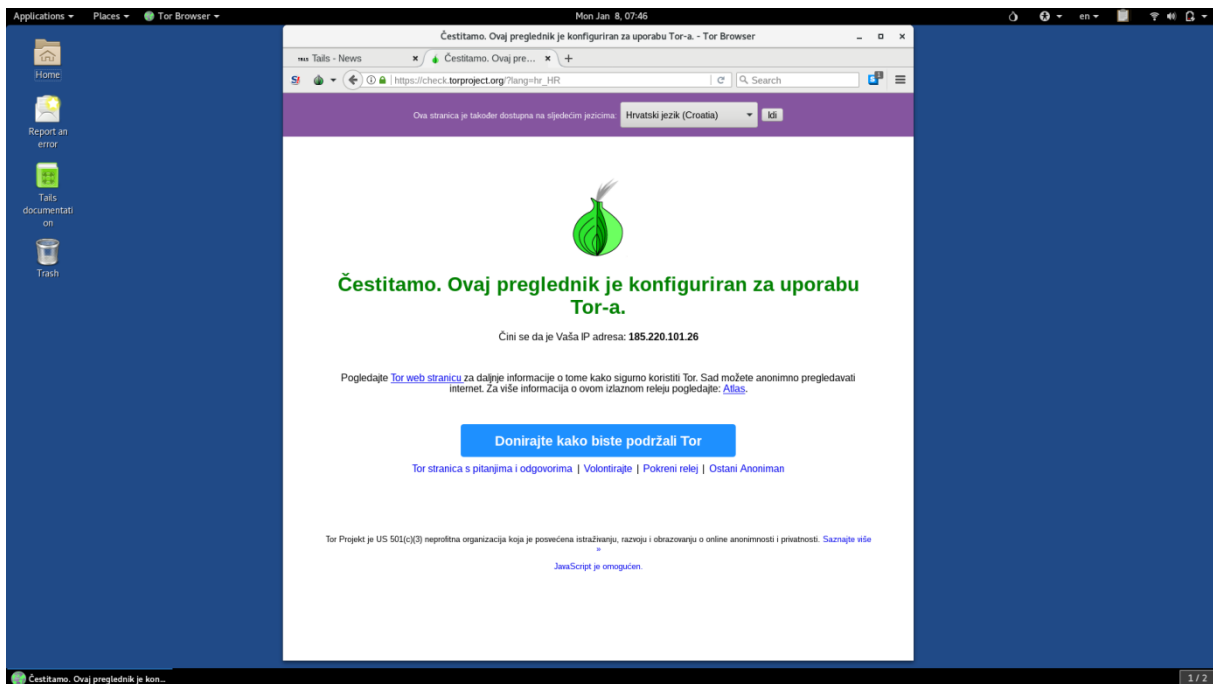
3.1.2 Korištenje Tailsa

Operacijski sustav Tails dolazi s brojnim programima za svakodnevno korištenje računala s naglaskom na sigurnost, privatnost i anonimnost. Neki od uključenih alata su:

- **Tor Browser** kao Web preglednik
- **Pidgin** kao sigurni *chat* program s konfiguriranim *Off-the-Record Messaging* (skraćeno OTR) protokolom za sigurnu komunikaciju
- **Thunderbird** (s **Enigmail** dodatkom za OpenPGP) za e-poštu
- **Electrum** kao softverski novčanik za Bitcoin (eng. *Bitcoin wallet*)
- **LibreOffice** kao skup uredskih programa (alternativa Microsoft Wordu, Excelu, PowerPointu...)
- **OpenPGP Applet** za šifriranje, dešifriranje, digitalno potpisivanje i provjeru digitalnih potpisa proizvoljnog teksta
- **OnionShare** za anonimno dijeljenje datoteka

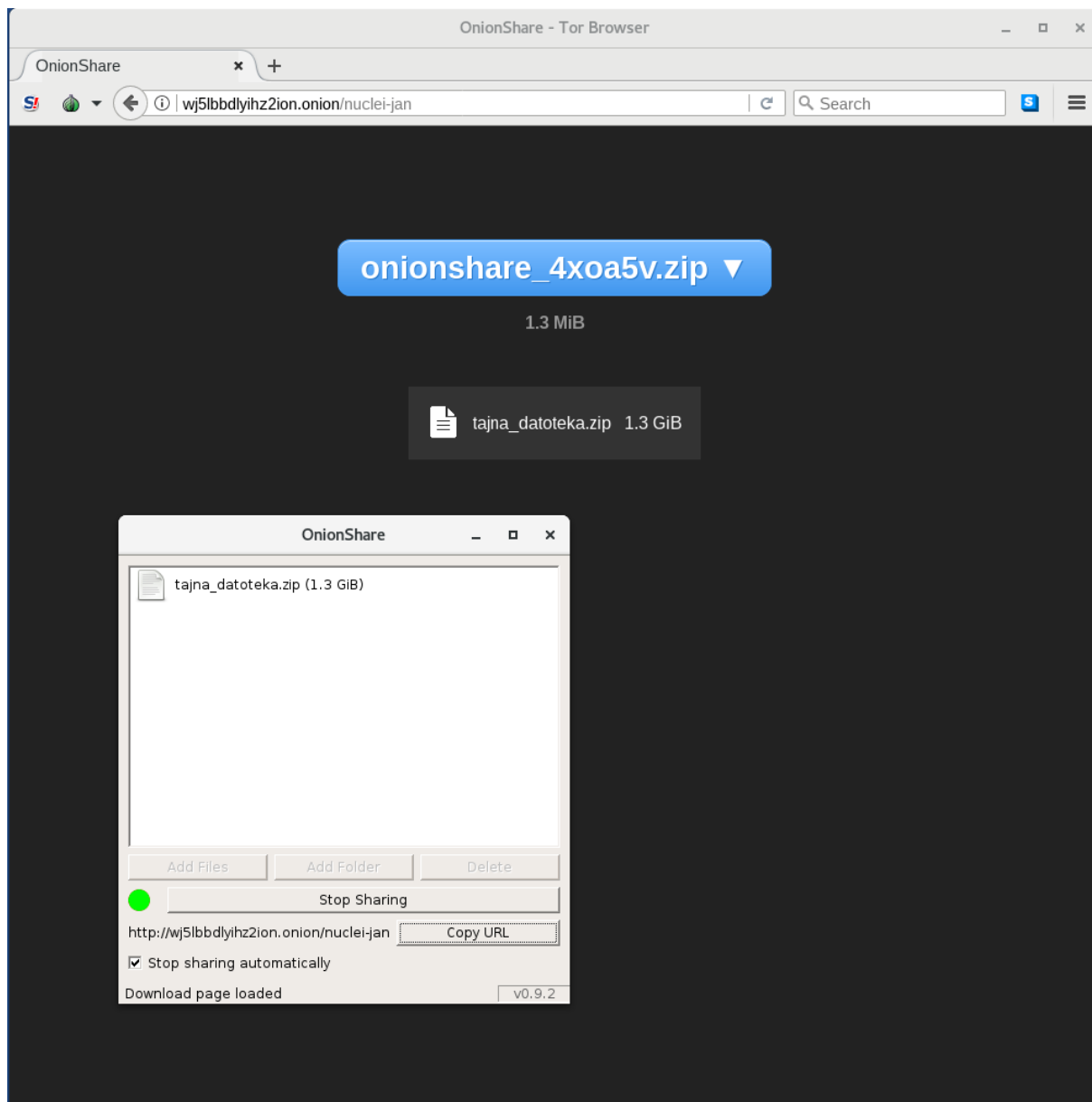
Detaljnije upute za korištenje ovih alata moguće je pronaći u [službenoj dokumentaciji](#) operacijskog sustava Tails.

Na slici 2 prikazan je Tor Browser otvoren unutar operacijskog sustava Tails. Otvorena je Web stranica na adresi <https://check.torproject.org/> kojom je moguće provjeriti je li Tor ispravno konfiguriran.



Slika 2 – Tor Browser otvoren unutar operacijskog sustava Tails

Na slici 3 prikazan je primjer korištenja alata OnionShare unutar operacijskog sustava Tails. To je alat koji stvara sakriveni servis kojem se može pristupiti kroz Tor mrežu (primjerice preko Tor Browsera) za anonimno dijeljenje datoteka.



Slika 3 – Dijeljenje datoteka pomoću alata OnionShare unutar operacijskog sustava Tails

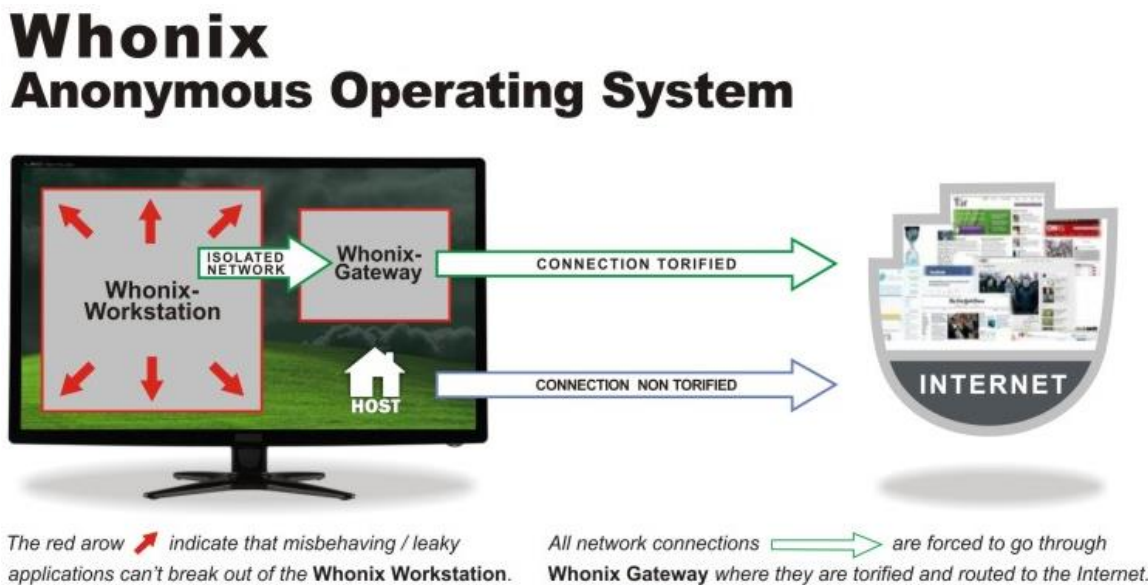
3.2 Whonix

Kao i Tails, Whonix je operacijski sustav koji za anonimnost koristi Tor mrežu. Također, jedan od ciljeva Whonixa je da **sav mrežni promet na sustavu putuje kroz Tor mrežu**. No u usporedbi s Tailsom, način na koji Whonix to postiže značajno se razlikuje.

Kako bi postigao navedeno, Whonix se sastoji od **dva dijela** (dva virtualna stroja):

1. Whonix radna stanica (eng. *Whonix workstation*) i
2. Whonix pristupnik (eng. *Whonix gateway*)

Korisnik koristi Whonix **isključivo kroz radnu stanicu** koja je mrežno spojena **samo na pristupnik**. Pristupnik je konfiguriran tako da sav promet s radne stanice putuje kroz Tor mrežu. Takva arhitektura osigurava da čak **ni radna stanica ne zna vanjsku IP adresu računala**. Zbog toga, za razliku od Tailsa, ni uspješan napad na radnu stanicu ne znači da je automatski kompromitirana anonimnost korisnika. Slika 4 iz dokumentacije Whonixa vizualno prikazuje i pojašnjava njegovu arhitekturu.



Slika 4 - vizualni prikaz i pojašnjenje arhitekture operacijskog sustava Whonix ([izvor](#))

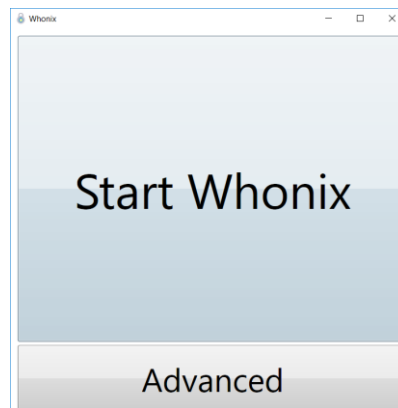
3.2.1 Instalacija

Kao što je navedeno u uvodu ovog poglavlja, Whonix se sastoji od dva virtualna stroja – jednog za pristupnik i jednog za radnu stanicu. Whonix je moguće instalirati na različite načine, uključujući izravno preuzimanje i korištenje slika virtualnih strojeva unutar alata VirtualBox te čak i [integracija u operacijski sustav Qubes](#).

No najjednostavniji način za Windows korisnike je korištenje [Whonix-Installer](#) programa. Pomoću njega, moguće je jednostavno instalirati Whonix kao program unutar operacijskog sustava Windows.

3.2.2 Korištenje

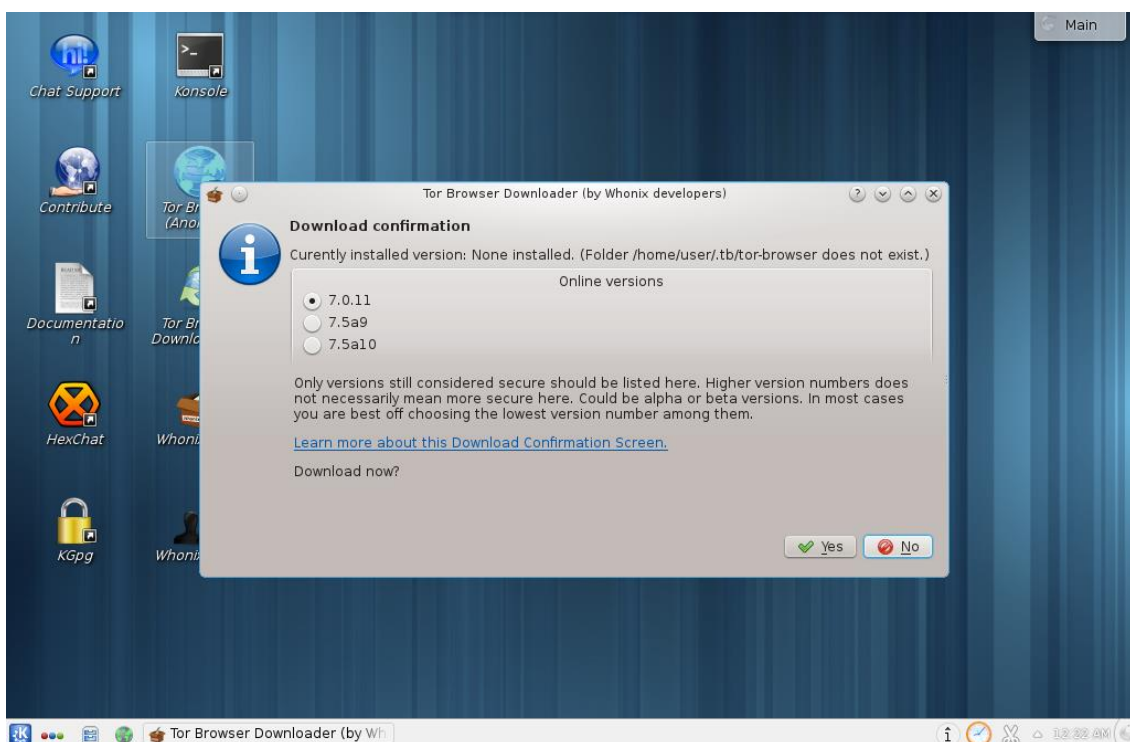
Whonix-Installer samostalno instalira alat *VirtualBox* te u njega učitava potrebne virtualne strojeve. Pokretanjem prečice *Whonix for Windows* na radnoj površini računala otvara se prozor prikazan na slici 5 unutar kojeg je moguće pokrenuti oba virtualna stroja klikom na *Start Whonix*.



Slika 5 – Prozor koji se otvara nakon pokretanja prečice *Whonix for Windows*

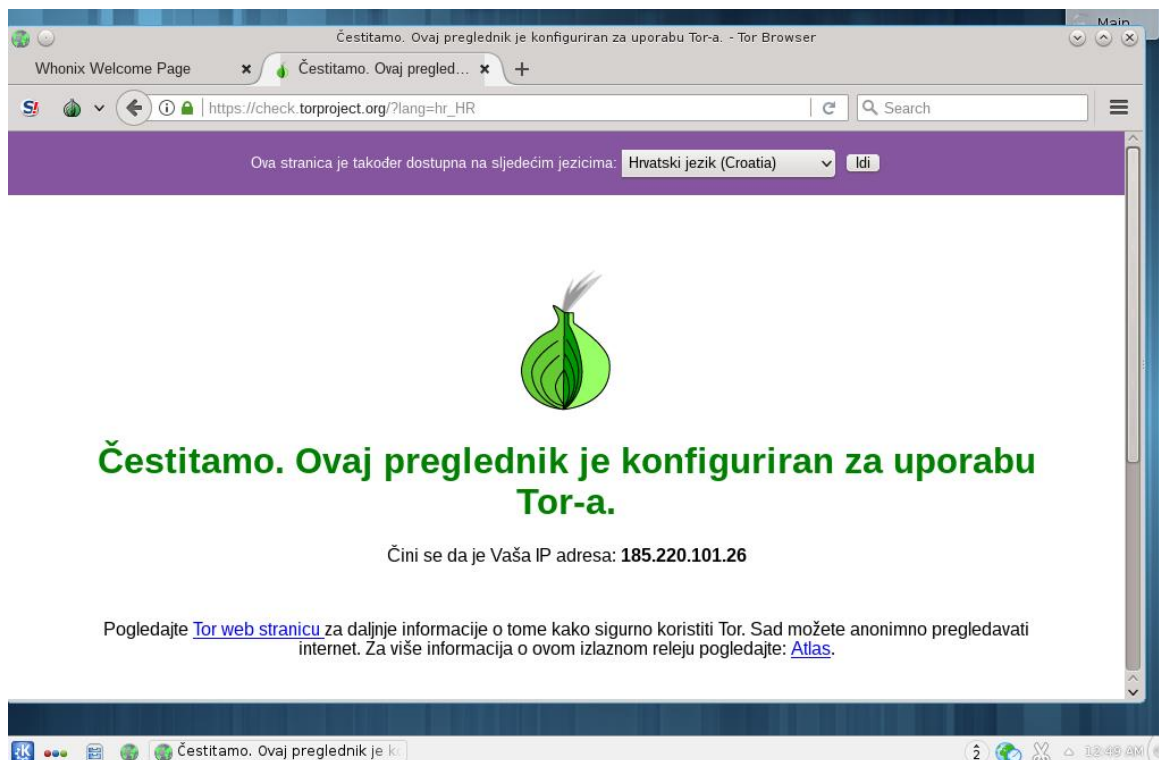
Prilikom prvog pokretanja pokrenut će se i čarobnjak koji vodi korisnika kroz podešavanje Whonixa.

Prije korištenja *Tor Browsera* unutar Whonixa potrebno ga je preuzeti te instalirati. Prilikom prvog otvaranja ikone *Tor Browsera* s radne površine, pojavit će se okvir u kojem se može odabrati inačica *Tor Browsera* za preuzimanje, kao što je prikazano na slici 6.



Slika 6 – Prozor za preuzimanje i instalaciju *Tor Browsera* unutar Whonixa

Nakon instalacije te pokretanja Tor Browsera, moguće je provjeriti ispravnost konfiguracije Tora posjetom Web stranice na adresi <https://check.torproject.org/> kao što je prikazano na slici 7.



Slika 7 – Tor Browser otvoren unutar operacijskog sustava Whonix

3.3 Konfiguracija vlastitog sakrivenog servisa

Ovo poglavlje namijenjeno je korisnicima koji imaju iskustva s konfiguracijom mrežnih poslužitelja, primjerice Web poslužitelja na kojem se temelji ovaj primjer. Ovdje će biti objašnjeno kako konfigurirati mrežni poslužitelj da bude dostupan unutar Tor mreže kao **Tor sakriveni servis**.

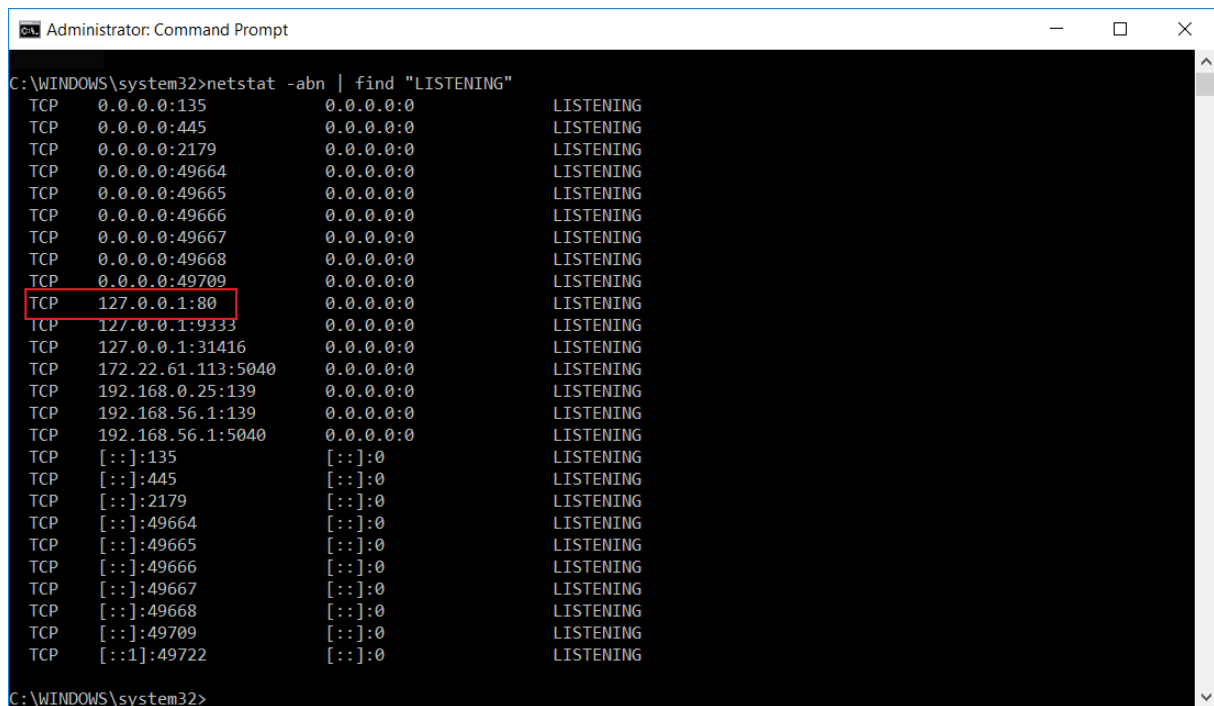
Preduvjet postavljanju sakrivenog servisa je da je konfiguriran i funkcionalan pristup Tor mreži, te da je prethodno konfiguriran poslužitelj, u ovom slučaju Web poslužitelj.

Kako bi se osigurala anonimnost, nužno je poslužitelj dodatno podesiti da mu se može pristupiti isključivo preko računala na kojem je on pokrenut, primjerice preko lokalne adrese 127.0.0.1. S obzirom na to da je Tor pokrenut na istom računalu, on će omogućiti da s poslužiteljem mogu komunicirati druga računala Tor mreže. Također, preporučljivo je da na računalu s Tor sakrivenim servisom općenito ne postoje nikakvi javno dostupni servisi kako to ne bi negativno utjecalo na anonimnost.

Unutar operacijskog sustava Windows, pokretanjem naredbene linije (*eng. Command prompt*) s administratorskim ovlastima te izvođenjem naredbe:

```
netstat -abn | find "LISTENING"
```

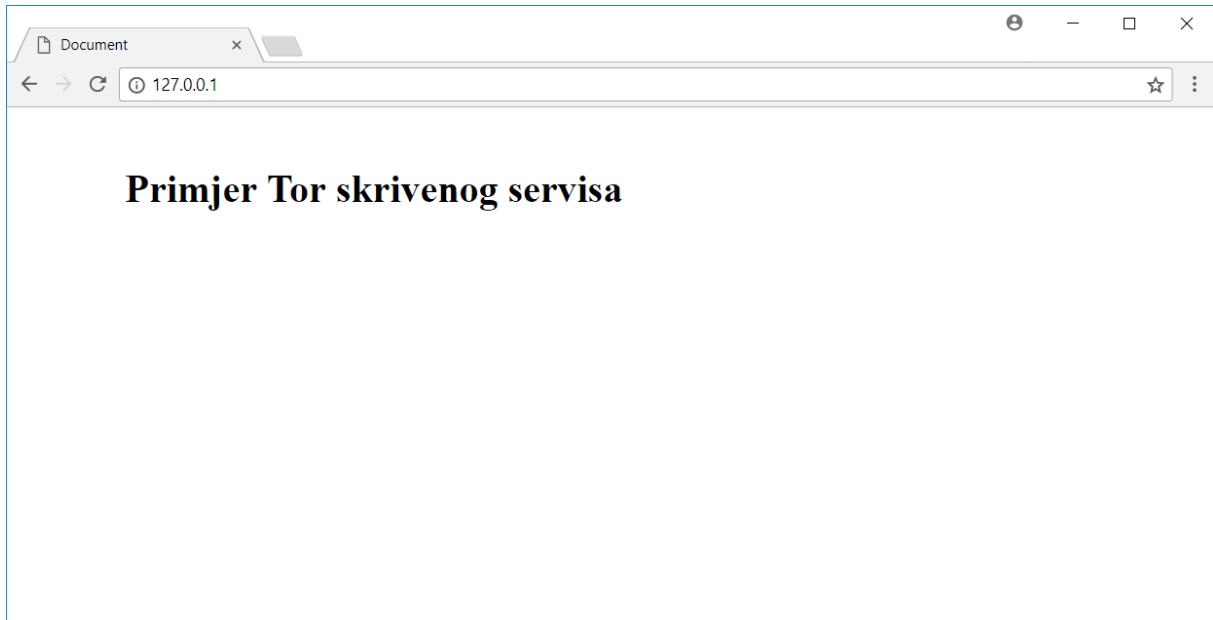
moguće je provjeriti dozvoljava li se pristup poslužitelju samo s istog računala. U ovom primjeru, Web poslužitelj postavljen je da sluša na priključku 80. Na slici 8 prikazano je kako se pokretanjem prethodno navedene naredbe vidi da poslužitelj prima zahtjeve samo na lokalnoj adresi 127.0.0.1. To je primjer ispravne konfiguracije – u slučaju neispravne konfiguracije, adresa povezana s priključkom 80 često bi bila 0.0.0.0, što bi značilo da je moguće izravno pristupiti Web stranici i preko Interneta, bez Tor mreže.



```
Administrator: Command Prompt
C:\WINDOWS\system32>netstat -abn | find "LISTENING"
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2179 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49709 0.0.0.0:0 LISTENING
TCP 127.0.0.1:80 0.0.0.0:0 LISTENING
TCP 127.0.0.1:9333 0.0.0.0:0 LISTENING
TCP 127.0.0.1:31416 0.0.0.0:0 LISTENING
TCP 172.22.61.113:5040 0.0.0.0:0 LISTENING
TCP 192.168.0.25:139 0.0.0.0:0 LISTENING
TCP 192.168.56.1:139 0.0.0.0:0 LISTENING
TCP 192.168.56.1:5040 0.0.0.0:0 LISTENING
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:2179 [::]:0 LISTENING
TCP [::]:49664 [::]:0 LISTENING
TCP [::]:49665 [::]:0 LISTENING
TCP [::]:49666 [::]:0 LISTENING
TCP [::]:49667 [::]:0 LISTENING
TCP [::]:49668 [::]:0 LISTENING
TCP [::]:49709 [::]:0 LISTENING
TCP [::1]:49722 [::]:0 LISTENING
C:\WINDOWS\system32>
```

Slika 8 – Rezultat izvođenja naredbe `netstat -abn | find "LISTENING"` prilikom konfiguracije Web poslužitelja – crvenom bojom označena je IP adresa na kojoj Web poslužitelj prima zahtjeve

Slika 9 prikazuje otvoreni Web preglednik na računalu na kojem je postavljen Web poslužitelj. Otvorena je adresa <http://127.0.0.1/> kojom je provjereno da Web poslužitelj ispravno poslužuje Web stranicu. U ovom trenutku Tor sakriveni servis još ne postoji – za sada je samo lokalno postavljen Web poslužitelj.



Slika 9 – Web preglednik otvoren na računalu na kojem je konfiguriran Web poslužitelj

Tor koristi konfiguracijsku datoteku *torrc* u kojoj se parametri rada Tor softvera konfiguriraju naredbama. Ako je Tor na Windows računalu instaliran kroz Tor Browser, datoteka *torrc* nalaziti će se na putanji *Browser\TorBrowser\Data\Tor\torrc* unutar direktorija gdje je Tor Browser instaliran.

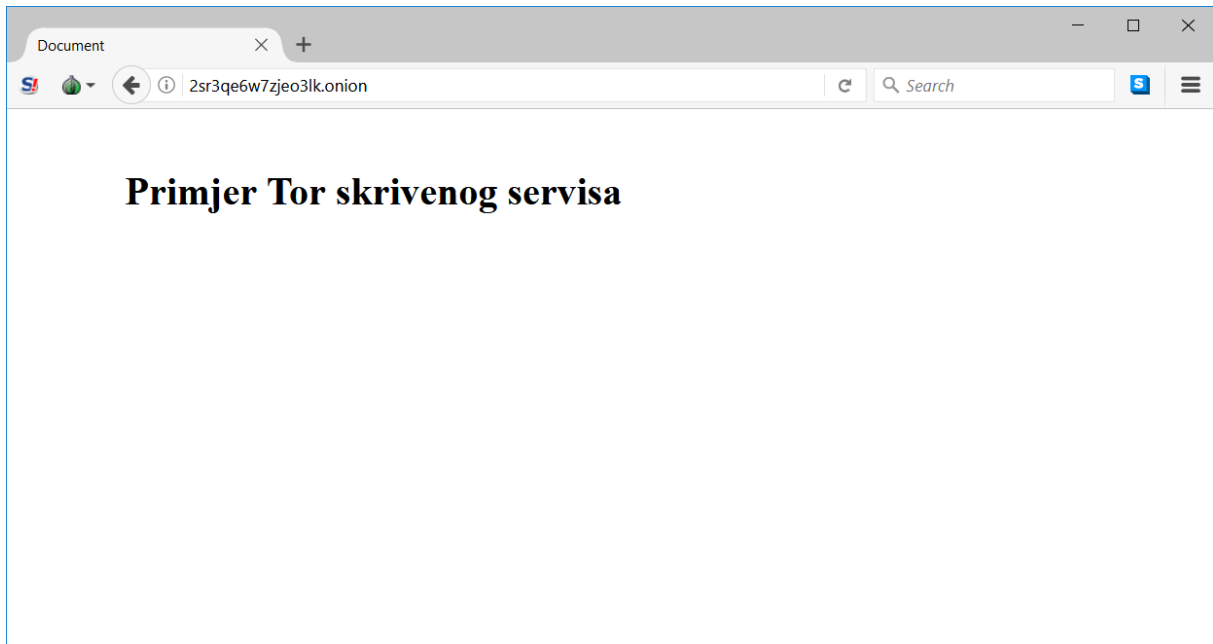
U tu datoteku potrebno je zapisati naredbe kako bi Tor registrirao novi sakriveni servis. U kontekstu ovog primjera, potrebno je zapisati sljedeće naredbe:

```
HiddenServiceDir C:\Users\korisnik\Documents\tor\hiddens_service  
HiddenServicePort 80 127.0.0.1:80
```

Direktorij nakon ključne riječi *HiddenServiceDir* je direktorij u koji će se spremiti konfiguracija Tor sakrivenog servisa. Prvi broj nakon ključne riječi *HiddenServicePort* je broj priključka na koji će se spajati korisnici Tor sakrivenog servisa, a 127.0.0.1:80 je IP adresa i priključak na kojem je lokalno pokrenut Web poslužitelj.

Tor će u ovom primjeru u direktoriju *C:\Users\korisnik\Documents\tor\hiddens_service* nakon prvog pokretanja stvoriti dvije datoteke: *hostname* i *private_key*. U datoteci *hostname* nalazi se generirana *.onion* domena sakrivenog servisa, a u datoteci *private_key* nalazi se privatni ključ koji se mora držati tajnim.

Slika 10 prikazuje kako se sada, otvaranjem Tor Browsera i upisivanjem *.onion* adrese sakrivenog servisa otvara Web stranica prethodno postavljenog Web poslužitelja.



Slika 10 – Tor Browser u kojemu je uspješno otvorena Web stranica novo konfiguriranog Tor skrivenog servisa

Ovdje je dan osnovni pregled postavljanja Tor skrivenog servisa, no ove upute ne pokrivaju sve načine zaštite od ugroza anonimnosti. Kako i mala greška može narušiti anonimnost poslužitelja, treba se dobro upoznati s relevantnim rizicima. Dobre početne točke za daljnje informiranje moguće je pronaći [ovdje](#) i [ovdje](#).

4 Zaključak

Tor je jedan od najboljih i najšire korištenih sustava za osiguravanje privatnosti i anonimnosti prilikom korištenja Interneta. Ispravnim korištenjem Tor mreže moguće je zamaskirati put mrežnog prometa te tako prikriti svoj identitet i aktivnosti na Internetu. Također, zbog načela rada Tor mreže moguće ju je koristiti i za zaobilaženje cenzure – ukoliko pružatelj mrežnih usluga blokira pristup nekoj Web stranici, čestu ju je i dalje moguće posredno posjetiti kroz Tor mrežu.

Zbog prethodno navedenih razloga, Tor je posebno koristan alat osobama koje žive u totalitarnim režimima gdje su cenzura i nadzor komunikacije uobičajeni. Kako bi zadržali kontrolu, totalitarni režimi često pokušavaju blokirati pristup Tor mreži. S tehničke strane, blokiranje se odvija na dva načina – putem IP adresa Tor čvorova te analizom prometa. Korištenjem Tor mosnih čvorova (eng. *Tor bridge relays*) i uklopnih prijevoznika (eng. *pluggable transports*) obično je moguće zaobići takve pokušaje blokiranja te se uspješno spojiti na Tor mrežu.

Većina korisnika koristi Tor kao zaštitu pri svakodnevnim oblicima korištenja Interneta – posjećivanje Web stranica, slanje elektroničke pošte te *chat/instant messaging* poruka. No, kroz Tor sakrivene servise, i pružatelji mrežnih usluga mogu osigurati svoju anonimnost odnosno anonimnost svojih mrežnih poslužitelja.

U konačnici, Tor služi i kao temeljna tehnologija na kojoj su izgrađeni drugi alati, kao što su operacijski sustavi Tails i Whonix. Prilikom njihovog korištenja, mrežni promet svih korištenih programa usmjeren je kroz Tor mrežu. Na taj način, osigurana je izrazito visoka razina privatnosti na prilično jednostavan način za krajnjeg korisnika.

5 Literatura

1. **Emin Çalışkan, Tomáš Minárik, Anna-Maria Osula.** Technical and Legal Overview of the Tor Anonymity Network. s.l. : NATO Cooperative Cyber Defence Centre of Excellence, 2015.
2. **Gunkarta.** Introducing Bastet, Our New Directory Authority . [Mrežno] [Citirano: 24. 1 2018.] <https://blog.torproject.org/introducing-bastet-our-new-directory-authority>.
3. **Chloe.** Tips for running an onion. [Mrežno] [Citirano: 24. 1 2018.] <https://labs.detectify.com/2016/04/05/tips-for-running-an-onion/>.
4. **Stockley, Mark.** Can you trust Tor's entry guards? [Mrežno] [Citirano: 24. 1 2018.] <https://nakedsecurity.sophos.com/2015/08/03/can-you-trust-tors-entry-guards/>.
5. **The Tor Project, Inc.** Tor Documentation. [Mrežno] [Citirano: 24. 1 2018.] <https://www.torproject.org/docs/documentation.html.en>.
6. **Wright, Jordan.** How Tor Works Part Three - The Consensus. [Mrežno] [Citirano: 24. 1 2018.] <https://jordan-wright.com/blog/2015/05/14/how-tor-works-part-three-the-consensus/>.
7. **Whonix.** Whonix Wiki. [Mrežno] [Citirano: 24. 1 2018.] https://www.whonix.org/wiki/Main_Page.
8. **Tails.** Tails Documentation. [Mrežno] [Citirano: 24. 1 2018.] <https://tails.boum.org/doc/index.en.html>.
9. **Riseup.** Tor Hidden (Onion) Services Best Practices. [Mrežno] [Citirano: 24. 1 2018.] <https://riseup.net/ca/security/network-security/tor/onionservices-best-practices>.