Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

IVAN JUGOVIĆ

DUBOKI WEB

Završni rad

Pula, rujan 2022.

Sveučilište Jurja Dobrile u Puli
Fakultet informatike u Puli

IVAN JUGOVIĆ

DUBOKI WEB

Završni rad

JMBAG: **0303061783**, redoviti student
Studijski smjer: Informatika
Znanstveno područje: Društvene znanosti
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija
Kolegij: Ekonomika informacijskih sustava
Mentor: izv.prof. dr.sc. Ivan Pogarčić

Pula, rujan 2022.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____, ovime izjavljujem da je ovaj završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio završnog rada nije napisan na nedopušten način, odnosno da ni/je prepisan iz kojega necitiranog rada, te da nijedan njegov dio ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine

IZJAVA

o korištenju autorskog djela

Ja, _____, dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj završni rad pod nazivom _____

_____

koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst, trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu sa Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

Sadržaj

1. UVOD

Živimo u svijetu u kojem su nam informacije dostupne u gotovo kakvom god obliku želimo. Tome je najviše pridonio razvoj umrežavanja servisa i ljudi diljem svijeta. U svojim počecima internet je bio privatna mreža kojoj su samo ovlašteni mogli pristupiti, no otkrivanjem prednosti koje je taj način slanja informacija mogao pridonjeti svijetu, internet je uskoro postao dostupan većini svjetske populacije. Internet, često oslovljen kao mreža svih mreža, sustav je koji se sastoji od glavne dvije razine sadržaja: *površinskog* i *dubokog weba*, dok se duboki dodatno dijeli i na *mračni web* koji je samo dijelić dubokog. Svakodnevno, kada pristupamo *webu,* koristimo se površinskim webom te je zapravo sve što vidimo putem konvencionalnih alata zapravo *površinski web*; od tražilica, oglasa pa sve do novinskih portala. *Duboki web* smatra se sadržajem kojem ne možemo pristupiti tako lako, njegov sadržaj je skriven od tražilica, većinom kao sadržaj u bazama podataka za koje je potreban ovlašten pristup, dok *mračni web* predstavlja mjesto na kojem se događaju aktivnosti kakve priliče nazivu „mračni."

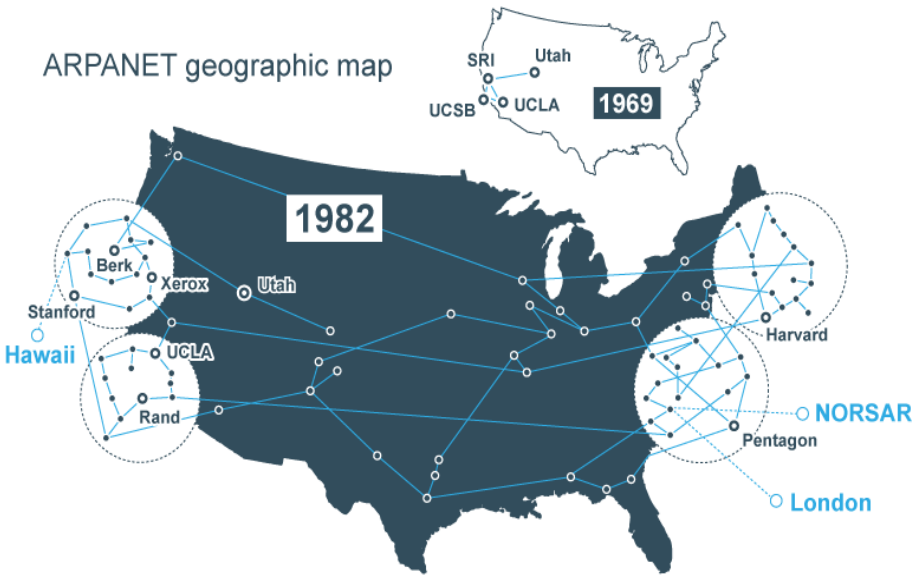
Pristup *mračnom webu* moguć je putem posebnih alata i protokola, najčešće povezan s terminom *TOR.* TOR kao mreža napravljena je po uzoru na ideju *Onion routinga*, tehniku u kojem je podatak omotan slojevima zaštite koje je potrebno postupno ukloniti kako bi se vidio željeni rezultat. Takav način usmjeravanja podatka putem skupine pravila, opisani u daljnjem tijeku rada, omogućuje korisnicima stvaranje potpune anonimnosti u korištenju interneta. Potreba za takvim tehnikama proizišla je iz sve većeg prometa na internetu te željama korisnika za povećanjem privatnosti koja se počela koristiti u krive svrhe. Gotovo sve usluge koje omogućuju zlouporabu anonimnosti dio su skrivenih *onion* usluga kao dio TOR mreže te pripadaju dijelu *mračnog weba*.

U ovom radu će na početku biti opisana kratka povijest razvoja interneta. U sljedećem poglavlju definiraju se razlike između vrsta *web* sadržaja te se otkrivaju načini ostvarivanja svake od vrsta. Glavni dio rada bazira se na proučavanju *Onion routinga* kroz uspoređivanje s tradicionalnom komunikacijom, analizu sigurnosti te način rada. Nakon ideje *Onion routinga,* prikazuje se stvarna implementacija u obliku TOR mreže te se analizira rad i sigurnost mreže. Posljednji dio rada sadrži informacije o *mračnom webu*, načinu pristupa te sadržaju koji prolazi putem njega.

2. POVIJESNI RAZVOJ INTERNETA

Internetom smatramo globalnu podatkovnu mrežu koja povezuje računala i mreže putem internetskog protokola (skraćeno IP) te ju kao takvu poznajemo od 90-tih godina prošlog stoljeća, a začeci razvoja sežu u 60-te godine.

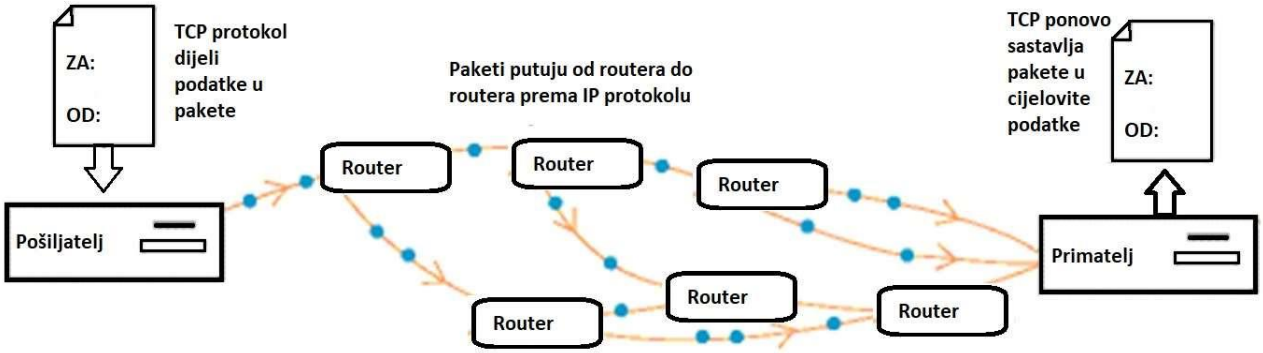
Prvi zapisi o internetu sežu u 1962. godinu kada je u dokumentu autora J. C. R. Licklidera predstavljen koncept „galaktične mreže" u kojoj bi kao danas računala vrlo brzo pristupala podacima te ih razmjenjivala. Pred kraj 60-tih, točnije 1969. osniva se ARPANET, rasprostranjena mreža na području SAD-a, koja je povezivala sveučilišta, ali i istraživačke centre. 1969. godine stvoreni su serveri, točnije njih četiri u američkim gradovima: Stanfordu, Los Angelesu, Santa Barbari i Utahu (Popović, 2002.).



Slika 1. Prikaz ekspanzije ARPANET-a u razdoblju 1969.-1982.
Izvor: https://portswigger.net/cms/images/e0/91/1afc66d7078e-article-arpanet-infographic-map.png

ARPANET je u svojim počecima imao vlastiti *host-to-host* protokol nazvan NCP (*Network Control Protocol*). Protokol je imao svoje nedostatke te je zbog manjka dokumentacije i nejasnoće, grupa istraživača na ARPANET-u održala konferenciju u Washingtonu 1972. te predstavila potencijale ovog sustava, od udaljene prijave do uređivanja tekstova preko veze. Poslije konferencije, mnogi drugi koji nisu bili dio zatvorenog sustava ARPANET-a imali su uvid u postojanje i mogućnosti komunikacije ovog tipa.

Odvojeno od ARPANET-a, tijekom 1973. godine postavljeni su posebni *serveri* u Londonu i u Norveškoj te se u daljnjem razdoblju širio broj nezavisnih servera diljem svijeta. Jedna od prijelomnih točaka u razvoju interneta vezala se uz pitanje spajanja različitih mreža u zajedničku komunikaciju diljem svijeta. NCP je bio ograničen na upravljanjem komunikacijom između *servera* koji su u istoj mreži te se nije moglo komunicirati s novim točkama diljem svijeta. Rješenje pitanja slanja podataka kroz različite mreže postao je TCP/IP protokol (*Transfer Control Protocol/Internet Protocol*). Njegov razvoj trajao je pet godina te je dovršen 1978. Glavni zadatak protokola jest prenijeti poruku u izvornom obliku od strane pošiljatelja do primatelja.



Slika 2. Pojednostavljeni prikaz TCP/IP protokola.

Izvor:

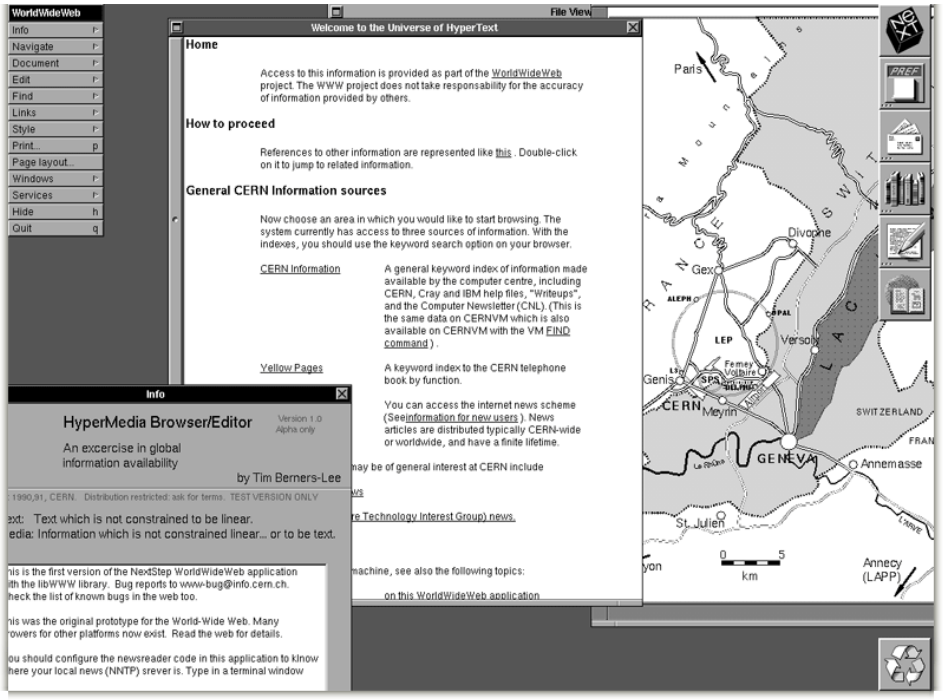
http://nevena.lss.hr/recordings/fer/predmeti/racfor/2018/seminari_2018_2019/lposilovic/seminar.pdf

Širenjem ARPANET-a i napretkom tehnologije sve se više računala moglo spojiti na mrežu. Takva situacija dovela je do sve više ovlaštenih i neovlaštenih upada na mrežu. Mreža je služila u istraživačke, ali i vojne svrhe, a vojska se tako odlučila odvojiti u MILINET, mrežu koja je bila zaštićena enkripcijom te kontrolom pristupa. Isto tako kao i vojska, znanstvenici su se odvojili u svoju posebnu mrežu NFTNET.

Tako se 80-tih godina javljao sve veći interes za otvorenom mrežom dostupnom svima. ARPANET je ugašena 1990. godine, kao i NFTNET 1995. godine. Gašenjem ovih mreža, začetnicama interneta kakvog danas poznajemo, internet je prešao iz privatnog u novu vrstu komunikacije dostupnu svima. Godine 1990. godine, Tim Berners-Lee u CERN-u u Švicarskoj izradio je sustav slanja informacija putem interneta kroz različita računala i operacijske sustave, a taj sustav nazvao je „*World Wide Web*" ili skraćeno WWW (Navarria, 2016.).

WWW je postao internetska usluga koja je postala javna 1994. godine. Ona omogućava pregled hipertekstualnih dokumenata koji sadrže multimedijske sadržaje, tekstove i slike, a identificiraju se pomoću *linkova* URL-a koji mogu biti povezani *hiperlinkovima*. Mrežni preglednici služe kao programi koji prikazuju takve dokumente (Gale Encyclopedia of E-Commerce, 2021.).

Na slici 3. prikazana je rekreacija originalnog izgleda WWW preglednika na računalu NeXT, koje je Tim Berners-Lee koristio u projektu.



Slika 3. Izgled prvog WWW preglednika.
Izvor: http://info.cern.ch/images/NextEditorBW.gif

Razvoj internetskih usluga kao što su WWW, e-pošta, prijenos podataka FTP te komercijalizacija interneta, dovelo je do rasta broja korisnika, ali i prometa. Godine 1995. godine broj korisnika iznosio je oko 16 milijuna ljudi te se rast nastavio eksponencijalno. Pred kraj 20. stoljeća, broj korisnika iznosio je 250 milijuna. Današnje brojke govore o tome kako je trenutno u svijetu 5 milijardi korisnika interneta. Globalni promet na internetu 1984. iznosio je samo 15 GB. Od početka do kraja 90-tih promet je skočio s 1 TB na 25 TB. Neke projekcije za 2020. prikazale su kako će promet na mjesečnoj bazi biti oko 160 EB (Sumits, 2015.) (Miniwatts Marketing Group, 2021.).

3. SADRŽAJ WEBA

3.1. PODJELA WEBA

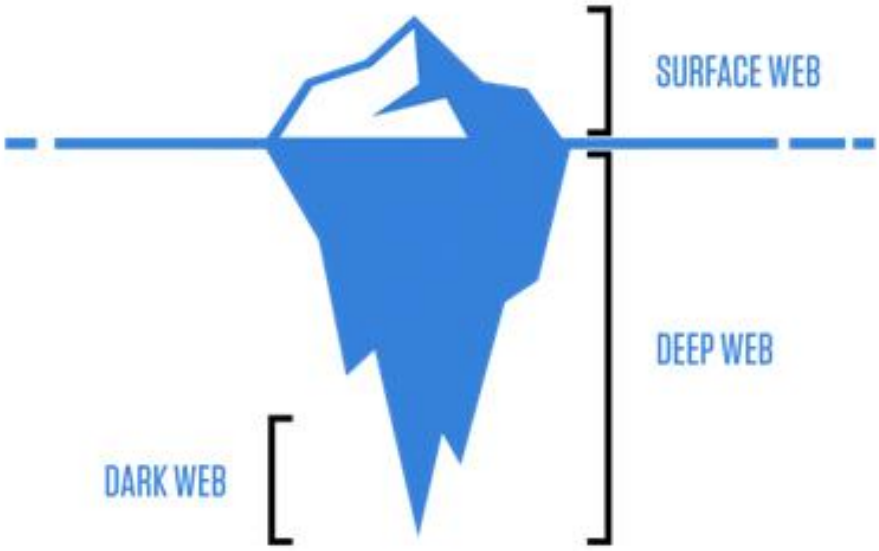
U poslijednje vrijeme često dolazi do miješanja termina „internet" i „*web*". *Web* je usluga koja se koristi na internetu, a omogućuje nam pristup sadržaju. S obzirom na pristup sadržaju, najjednostavnija je podjela *weba* na dva glavna dijela:

- površinski (eng. *surface web*)
- duboki (eng. *deep web*) kojeg još dijelimo na mračni (eng. *dark web*)

Sadržaj koji pretražujemo putem popularnih tražilica kao što su Google, Bing, itd., pripadaju *površinskom webu*. Drugi dio *weba*, onaj *duboki,* tražilice ne indeksiraju njegov sadržaj zbog sigurnosnih, ali i tehničkih razloga. *Duboki web* sadrži informacije baza podataka kompanija, akademskih i znanstvenih istraživanja, sadržaj *e-mail* računa, društvenih mreža, bankovnih računa te zdravstvene i pravne zapise. Popularne tražilice ne mogu vratiti ovakav tip podatka korisniku jer one nisu povezane, kao što je navedeno ranije, najviše zbog sigurnosti. Kako bi se pristupilo sadržaju *dubokog weba* potrebno je tražiti sadržaj na tražilicama koje komuniciraju s bazama podataka kao što su npr. Google Scholar ili Google Patents (Kolb, 2020.).

Mračni web je djelić *dubokog weba*. Sadržaj *mračnog weba* skriven je pa mu je nemoguće pristupiti s osnovnim mrežnim preglednicima. Korisnici, kao i autori sadržaja na *mračnom webu* su anonimni i skriveni. *Mračni web* koristi se u svrhu dijeljenja podataka u anonimnosti, što je i glavni atribut na kojem se zasniva ovaj dio *weba*. Naziv "mračni'' dobio je zbog tendencije korištenja *weba* u krive svrhe. U ovom dijelu *weba* događaju se nelegalne stvari, od krađa identiteta do prodaje oružja. U posljednje vrijeme, *mračni web* nije dio samo nelegalnih akcija. Pojavljuje se značajan broj stranica vezanih za ljudska prava, novinarstvo i političke prosvjede. Razlog tomu svakako je anonimnost koju *mračni web* nudi korisnicima. Pristupanje *mračnom webu* nije zabranjeno, ali doticaj s kriminalnim radnjama zakonski je zabranjen (Susuri, 2019.).

Mračni web je sadržaj dostupan na *Darknetu*, koji je privatna računalna mreža stvorena na internetu. Za pristup sadržajima *mračnog weba* potrebni su posebni programi i protokoli, a više o njima biti će objašnjenjo u poglavlju 4.



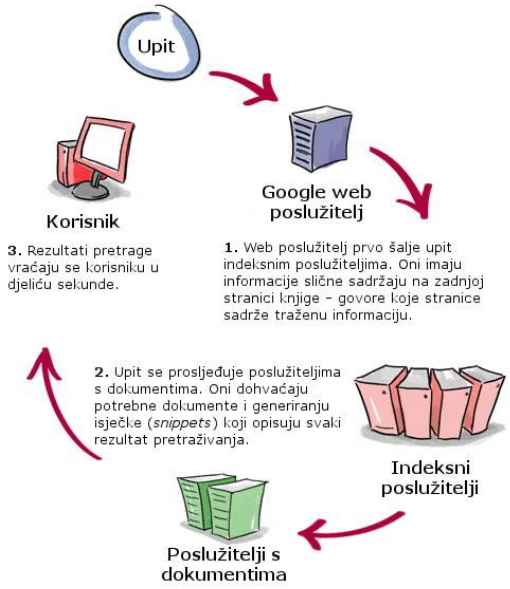
Slika 4. Ilustracija podjele weba.
Izvor: https://www.networkboxusa.com/what-is-the-dark-web/

Često se podijela predstavlja kao santa leda gdje je vidljivi dio sante leda *površinski web*, a ostatak *duboki*. Ilustracija je prikazana na slici 4. Sama ilustracija sante leda daje do znanja kako je *duboki web* znatno veći od *površinskog*. Projekcije prikazuju kako je *površinski web*, onaj kojeg koristimo svakodnevno, samo 5% dio ukupnog *weba*. Ostatak je dio *dubokog,* a samo mali dio *dubokog* je dio *mračnog weba* (do 5%) (Kolb, 2020.).

3.2. INDEKSIRANJE SADRŽAJA

Indeksiranje je proces u kojem tražilice organiziraju informacije prije pretraživanja kako bi omogućile brz odgovor na upit od strane korisnika.

Tražilice koriste automatizirane softvere kako bi analizirali *web* stranicu koju će uključiti u rezultate pretraživanja. Autori *web* stranica mogu prijaviti tražilicama svoje stranice kako bi ih tražilice onda analizirale. Automatizirani softveri, koji se nazivaju „mrežni pauci" prilikom analize indeksiraju i dodatne poveznice na *web* stranicama. Tražilice stoga, neprekidno indeksiraju stranice iz razloga mogućih promjena sadržaja na istima (Sherman & Price, 2007.). Na slici 5. vidljiv je proces koji tražilica odrađuje kako bi odgovorila na zahtjev korisnika.



Slika 5. Ilustrirani prikaz procesa pretraživanja na tražilici.

Izvor: https://www.info-kon.hr/wp-content/uploads/2017/02/20170211-kako-radi-google-i-ostale-trazilice2.jpg

3.2.1. NEVIDLJIVI WEB

Nevidljive stranice na *webu* sastoje se od sadržaja koje glavne tražilice ne mogu pronaći. Broj takvih stranica u odnosu na one koje se mogu pronaći u stalnom je rastu. Tablica 1. prikazuje razloge zbog kojih mrežni pauci ne mogu indeksirati određenu vrstu sadržaja.

Tablica 1. Vrste nevidljivih sadržaja i razlog neindeksiranja (Sherman & Price, 2007.).

Vrsta sadržaja	Razlog
Odspojena/nepovezana stranica	Mrežni pauk nema vezu po kojoj može pronaći stranicu
Stranica sastavljena u većini od slika, audiozapisa i videozapisa	Nedostatak tekstualnog objašnjenja
Stranica sastavljana u većini od .pdf datoteka, programa te kompresiranih datoteka	Zanemareno zbog pravnih razloga
Sadržaj u relacijskim bazama podataka	Mrežni pauk ne može ispuniti potrebne podatke za Pristup
Sadržaj u stvarnom vremenu	Brzo mijenjanje sadržaja
Dinamično kreiran	Mogućnost zamki za mrežne pauke

U Mansourianovoj studiji (2006.) *„nevidljivi web"* je podijeljen na: neprozirni, privatni, vlasnički te uistinu nevidljivi.

U ***neprozirnom webu***, sadržaj je takvog tipa da ga tražilice mogu obraditi i indeksirati, ali zbog sljedećih razloga to nije moguće:

- dubina dohvaćanja stranica od strane mrežnih paukova,
- učestalost dohvaćanja sadržaja,
- maksimalan broj rezultata,
- nepovezanost linkova.

Dubinom dohvaćanja stranica smatraju se neprikazane stranice u tražilicama zbog troškova indeksiranja ili ukoliko mrežne stranice sadrže mnogo podstranica, one u većini slučajeva neće biti prikazane. Učestalost dohvaćanja sadržaja ovisi o tendenciji promjena sadržaja na *webu*, a pauci će zbog tih promjena u određenim periodima vraćati i provjeravati stranice na kojima su moguće promjene. Nove stranice mogu biti dio *nevidljivog weba* iz razloga jer postojeće stranice upućuju na nove. Tražilica ima svoje limite koji joj određuju količinu sadržaja koju mogu prikazati te zbog toga limit utječe na vidljivost sadržaja. Limit se kreće između 200 i 1.000 rezultata pretraživanja. Sav ostatak sadržaja je dio *nevidljivog weba*. Ukoliko stranica ima nepovezane *linkove* ili ne postoji *link* za istu, tada ona ostaje dio *nevidljivog weba*.

Privatni web čine stranice koje su isključene iz rezultata tražilica iz određenog razloga. Većinom je taj razlog sigurnost. Stranice ovakvog tipa traže prijave putem korisničkog imena i lozinke. Druga mogućnost su *robots.txt* datoteke koje paucima ne dopuštaju pristup stranici. Treća mogućnost su meta oznake koje paucima omogućuju pristup glavi stranice.

Na slici 6. prikazan je sadržaj *robots.txt* datoteke. *User-agent* linija naređuje pauku kako mora pratiti naredne instrukcije. Pomoću znaka „*" naređuje se da svi pauci moraju pratiti instrukcije. Svaka linija u kojoj je naznačeno *„Dissalow*" zabranjuje pristup sadržaju od strane mrežnih paukova. Primjer koji je prikazan dio je direktorija na serveru Los Angeles Timesa (Sherman & Price, 2007.).

```
User-agent: *
Disallow: /RealMedia
Disallow: /archives
Disallow: /wires/
Disallow: /HOME/
Disallow: /cgi-bin/
Disallow: /class/realestate/dataquick/dqsearch.cgi
Disallow: /search
```

Slika 6. Primjer robots.txt datoteke (Sherman & Price, 2007.).

Na slici 7. prikazan je način skrivanja sadržaja putem ubacivanja *meta tagova* u glavu HTML dokumenta. Ubacivanjem *meta tag* instrukcije "noindex" u glavu dokumenta, onemogućuje se pristup mrežnim paucima.

```
<html>
<head>
<title>Keep Out, Search Engines!</title>
<META name="robots" content="noindex, nofollow">
</head>
```

Slika 7. Primjer "noindex" meta tag instrukcije (Sherman & Price, 2007.).

Glavna razlika između *robots.txt* datoteke i "noindex" instrukcije jest ta da je instrukcija specifična za stranicu, dok datoteka može štititi pojedine stranice, grupe podataka ili datoteke na stranici.

U ***vlasnički web*** spadaju stranice za koje je potreban internetski račun koji može biti besplatan ili plaćen. Takvi mrežni servisi imaju svoje uvjete korištenja te mrežni pauci nemaju informacije vezane za pristup računima, a time im se tako onemogućuje indeksiranje sadržaja (Sherman & Price, 2007.).

Vrste sadržaja ***uistinu nevidljivog weba*** i razlozi zbog kojih su nevidljivi prikazani su u Tablici 1.

4. KONCEPTI ANONIMNOSTI NA INTERNETU

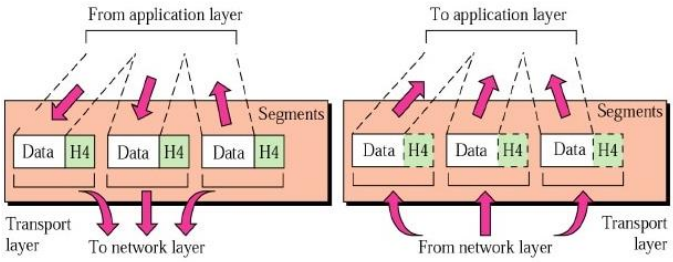
Porastom broja korisnika koji se koriste internetom doveo je do veće potražnje za servisima koji osiguravaju veću anonimnost. Anonimnost daje sigurnost korisnicima kako njihovi podaci i tragovi koje ostavljaju na internetu neće biti vidljivi nikome osim njim. Svjedoci smo kako sve više organizacija prati svoje korisnike te je cenzura sadržaja svakog dana u porastu. Upravo zbog navedenih razloga stvorene su tehnike omogućavanja anonimnosti na internetu.

4.1. *ONION ROUTING*

Onion routing je ideja ili tehnika ostvarivanja veće razine anonimnosti na internetu. Veća razina anonimnosti u ovom načinu omogućuje se slanjem poruke kroz više čvorova, gdje svaki čvor dešifrira dio poruke. Više čvorova i svako dešifriranje nalikuje luku koji se sastoji od više slojeva. Upravo zato je ovaj način usmjeravanja dobio naziv po luku. *Onion routing* je jedan od najpoznatijih i djelotvornih tehnika usmjeravanja za svrhu koju se koristi. Razvoj *Onion routinga* započet je sredinom 1990-ih u Američkom Pomorskom Istraživačkom Laboratioriju kako bi se zaštitila komunikacija obavještajnih službi na mreži. Godine 1998., *routing* je patentirala vojska (Reed, et al., 1997.).

4.1.1. PROBLEM STANDARDNE KOMUNIKACIJE

Model komunikacije ISO-OSI biti će baza za shvaćanje *onion routinga*. Model ISO-OSI sastoji se od najnižeg do najvišeg sloja: fizički, podatkovni, mrežni, transportni, sjednički, prezentacijski i aplikacijski. Proces primanja i slanja podataka je obrnuti, kod slanja podataka proces ide od najvišeg do najnižeg sloja. Poruka se prenosi putem fizičkog sloja u binarnom obliku koja se na odredištu dekompozira obrnutim putem od slanja. Slojevi kojima je glavni zadatak komunikacija dvaju točaka su transporni i mrežni. Transportni usmjerava podatak, a mrežni omogućuje pouzdanu uslugu. Na slici 9. prikazano je kako transportni i mrežni slojevi, koji su glavni fokus problematike usmjeravanja, dodavaju na poruke svoja zaglavlja. Zaglavlja na poruku, dakako dodavaju i ostali slojevi u komunikacijskom modelu (Day & Zimmermann, 1984.) (Pralas, 2008.).



Slika 8. Prikaz transportnog i mrežnog sloja.
Izvor: https://www.slideshare.net/abidshahzad/osi-model-1291761

Korisne informacije koje sadrže mrežni i transportni sloj su izvorište i odredište paketa te informacije o priključnim programima. Put poruke između dva čvora koji nisu dio iste mreže ide putem više čvorova koji nikad nije isti. Prikazani put zahtjeva za stranicom "unipu.hr" prikazan je na slici 10., a koji je moguć utipkavanjem naredbe "tracert [domena stranice]" u terminalu sustava.

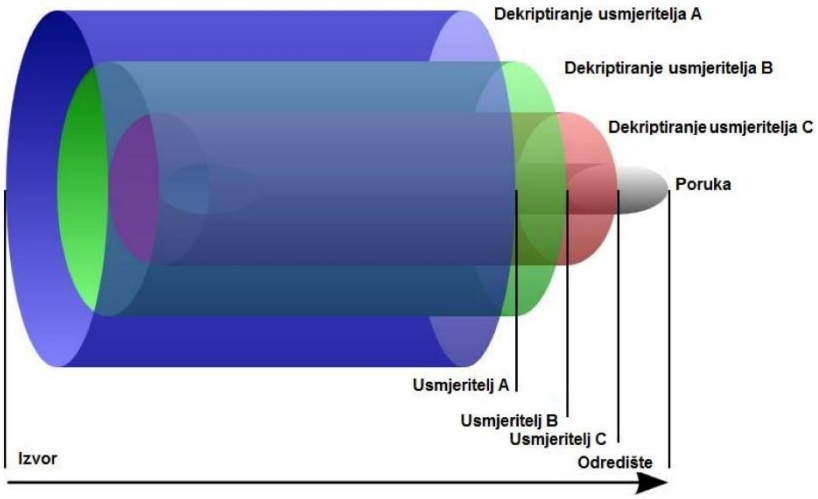
```
traceroute to unipu.hr (31.147.205.115), 64 hops max, 52 byte packets
 1  broadcom.home (192.168.1.1)  7.183 ms  4.144 ms  2.928 ms
 2  100.115.0.1 (100.115.0.1)  14.643 ms  14.510 ms  16.243 ms
 3  100.64.0.85 (100.64.0.85)  18.800 ms  17.777 ms  18.446 ms
 4  * * *
 5  dh120-77.xnet.hr (83.139.120.77)  25.527 ms  18.163 ms  17.932 ms
 6  carnet.cix.hr (185.1.87.65)  17.690 ms  20.134 ms  19.047 ms
 7  * * *
 8  * * *
 9  * * *
10  pellicus.unipu.hr (31.147.205.115)  110.499 ms  126.526 ms  142.742 ms
```

Slika 9. Prikaz puta paketa između osobnog računala i unipu.hr stranice.
Izvor: vlastito djelo

Prateći putanju paketa jasno je vidljivo kako paket prolazi kroz mnoštvo usmjerivača (čvorova) koji mogu biti ranjivi i praćeni, što od strane pružatelja mrežne infrastrukture do neovlaštenih korisnika koji ukoliko poruke nisu zaštićene mogu pročitati sadržaj, početnu i odredišnu adresu.

4.1.2. NAČIN RADA

Rješenje navedenom problemu predstavlja *onion routing* kod kojega je situacija takva da poruka putuje kroz nepredviđene usmjerivače ili posrednike te je poruka kriptirana kriptografijom javnog i privatnog ključa, a iz tog razloga posrednik ne može čitati poruku. Fleksibilnost ove tehnike je ta da omogućuje anonimnost ukoliko postoje kompromitirani usmjerivači unutar mreže jer svaki usmjerivač dekriptira samo dio poruke. Jasno, mogućnost napada je moguća ukoliko napadač poznaje sve usmjerivače u mreži, ali mogućnost toga je vrlo mala, zbog nepredviđenosti usmjerivača između početne i krajnje točke. *Onion* (eng. luk) u ovoj tehnici naziv je za poruku koja sadrži podatke koji su kriptirani javnim ključevima od strane svakog usmjerivača, kako bi ostali usmjerivači mogli nastaviti dekriptirati. U nastavku su navedeni uvjeti ostvarivanja ovakve komunikacije.



Slika 10. Prikaz strukture *onion routinga* i načina dekriptiranja.
Izvor: https://www.cis.hr/files/dokumenti/CIS-DOC-2012-09-061.pdf

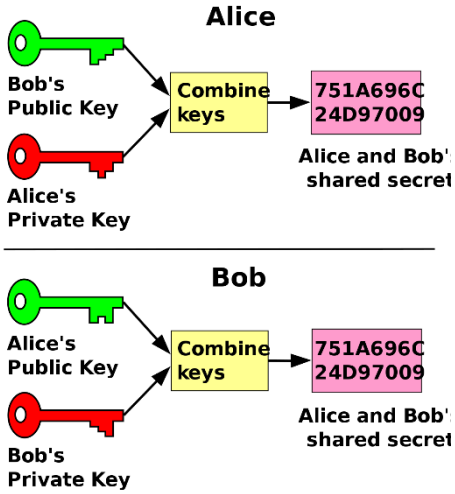
Uvjeti ostvarivanja navedene komunikacije putem nepredviđenih usmjerivača:

1. Korisnik koji šalje poruku kontaktira čvor koji sadrži informacije o usmjerivačima koji mogu prosljeđivati poruke, odabiru se čvorovi koji tvore put ili lanac prema primatelju. Niti jedan unutarnji čvor u lancu nema informacije o broju čvorova u lancu i svojoj poziciji u lancu.
2. Korisnik kriptira poruku putem javnog ključa za prvi čvor u lancu. Poruka sadrži: ID lanca koji je različit od ID ostalih stvorenih lanaca, zahtjev za uspostavom lanca komunikacije i

korisničku polovicu Diffie-Hellman rukovanja koji je tehnika izmjene kriptografskih ključeva između sudionika.

3. Prvi čvor u lancu ili ulazni čvor korisniku odgovara nekriptiranom porukom koja sadrži: drugu polovicu Diffie-Hellman rukovanja i sažetu vrijednost dijeljene tajne.
4. Kada korisnik i ulazni čvor imaju dijeljenu tajnu, mogu koristiti simetrično kriptiranje podataka.
5. Nakon 4. koraka, korisnik ostvaruje komunikaciju sa sljedećim čvorom slično kao i s ulaznim.
6. Navedeni čvor odgovara ulaznom čvoru kao u 3. koraku.
7. Ulazni čvor obavještava korisnika kako je komunikacija sa sljedećim čvorom ostvarena te mu šalje tajnu i dio Diffie-Hellman rukovanja. Ovim događajem korisnik i idući čvor u lancu imaju uspostavljenu tajnu koja im koristi za komunikaciju (cis.hr, 2012.).

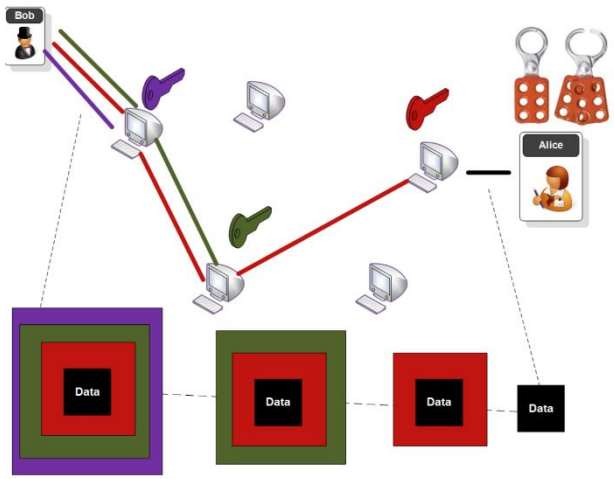
Vidljivo je kako je tehnika ostvarivanja čvorova u lancu skalabilna. Uspostavljanje lanca označava mogućnost i sigurnost anonimnog slanja podataka.



Slika 11. Pojednostavljeni prikaz dijeljenja Diffie-Hellman razmjene ključeva (rukovanja).
Izvor: https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange#/media/File:Public_key_shared_secret.svg

U Diffie-Hellman rukovanju koristimo primjer dvoje sudionika u komunikaciji kroz jednog bez posrednika. Neka su sudionici A i B, u prvoj iteraciji sudionici A i B generiraju svoje privatne ključeve pA i pB. U drugoj iteraciji pomoću privatnog ključa sudionici generiraju svoje javne ključeve kA i kB. Kada sudionici imaju spremne privatne i javne ključeve putem javnog

kanala razmjenjuju javne ključeve. U trenutku kada sudionici imaju tuđe javne ključeve kreću u računanje zajedničke tajne. Ostvarivanjem zajedničke tajne sudionici mogu sigurno komunicirati. Na slici 11. prikazan je pojednostavljeni model prethodno opisanog.



Slika 12. Prikaz onion routinga s razmjenom ključeva.
Izvor: https://asecuritysite.com/encryption/curve

Primjer prijenosa poruke u *onion routingu* s tri lanca (ulazni, srednji i izlazni čvor):

Slika 13. Struktura poruke sa HTTP zahtjevom.
Izvor: https://www.cis.hr/files/dokumenti/CIS-DOC-2012-09-061.pdf

Poruka je složena tako da se u crvenom području nalazi podatak kriptiran tajnom između korisnika i prvog čvora. Shodno tome, zeleni dio predstavlja tajnu srednjeg čvora i

korisnika, dok žuto označen čvor predstavlja tajnu između korisnika i zadnjeg čvora u lancu. Dekriptiranjem poruke ulazni čvor vidi poruku u obliku na slici 14. Kako je komunikacija uspostavljena ranije, čvorovi znaju kojim smjerom trebaju prosljeđivati poruku dalje u lancu.

Slika 14. Poruka nakon postupka dekriptiranja prvog čvora.
https://www.cis.hr/files/dokumenti/CIS-DOC-2012-09-061.pdf

Dekriptiranjem srednjeg sloja, srednji sloj vidi poruku u obliku na slici 15. te on poruku u takvom obliku šalje izlaznom čvoru koji može pročitati sadržaj poruke (u ovom slučaju HTTP protokol).

Slika 15. Poruka nakon postupka dektiptiranja drugog čvora (cis.hr, 2012.).

Nakon što je drugi čvor dekriptiran, izlazni čvor nastavlja komunikaciju, zahtjeva dohvat mrežnog mjesta te očekuje odgovor od poslužitelja na koji je poslao zahtjev. Poslužitelj odgovara izlaznom čvoru na način slanja HTTP odgovra sa HTML kôdom u sadržaju. Izlazni čvor kriptira poruku zajedničkom tajnom koju imaju on i korisnik te se poruka suprotnim smjerom od dolaska vraća prema korisniku. Kako bi korisnik došao do sadržaja mora tri puta s tri različita ključa čvorova u lancu dektriptirati poruku (cis.hr, 2012.).

4.1.3. SIGURNOST *ONION ROUTINGA*

Višestruko kriptiranje sadržaja povećava razinu sigurnosti slanja poruke kroz mrežne kanale. Kako bi se poruka u ovakvom tipu protokola htjela kompromitirati, tada napadač treba znati sve ključeve između čvorova. Višestruko kriptiranje onemogućava dekriptiranje bez poznavanja svih ključeva. Napadač može uspjeti, ukoliko dođe do ključa za jedan čvor, dekriptirati dio poruke, ali ne i nju u cijelosti. Većinom može doći do sadržaja ili mjesta odredišta i mjesta slanja, ali vrlo teško do objedinjenih informacija. Posrednici ili routeri najvažniji su dio *onion routinga* jer bez njihovog postojanja slanje poruka ovim načinom nije moguć. Posrednici su prilagođeni te znaju na koji se način vrši komunikacija unutar mreže.

Osim sigurne komunikacije unutar mreže, *onion routing* omogućuje logičko sakrivanje usluga. Fizičko sakrivanje može se realizirati bez *onion routinga* (OR) tako da se usluga spremi na poslužitelj te se sakrije informacija o pripadnosti poslužitelju. Logičko sakrivanje je omogućeno putem posrednika (OR) koji omogućavaju pristup usluzi te je računalo koje sadrži uslugu logički sakriveno od korisnika (inače, usluzi se pristupa putem IP adrese).

Zbog podužeg procesa koje nosi ovaj način *routinga*, vremenska analiza praćenja čvora može otkriti pripadnost paketa korisnicima. Na primjer, praćenjem čvora koji nije u prometnom opterećenju, putem vremenske analize moguće je povezati ulaznu poruku s izlaznom. Mogućnost rješenja ovog problema jest implementiranje spremnika na čvoru koji prosljeđuje poruku tek nakon što se spremnik napuni. Druga vrsta praćenja je moguća u slučaju otpadanja ili kvarenja čvorova (eng. *intersection attacks*). U tom slučaju, čvor nema usmjerivačku vezu te je analiza prometa omogućena (cis.hr, 2012.).

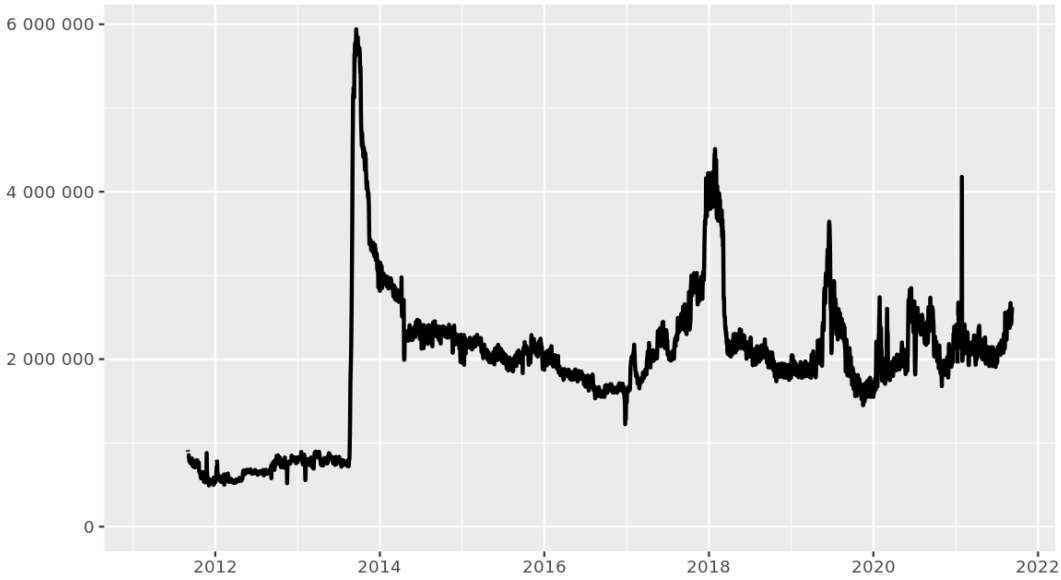
Poznat je problem izlaznog čvora u *onion routingu* jer je on najnesigurniji od cijelog lanca. Ukoliko napadač ima pristup izlaznom čvoru, može pročitati poruku. SSL protokol omogućuje rješavanje ovog problema u kojem se sadržaj dodatno kriptira tako da ni izlazni čvor nema pristup sadržaju.

4.2. TOR

TOR (skraćenica od *The Onion Routing*) najpoznatiji je program koji se temelji na ideji opisanoj u poglavlju 4.1. te je predstavnik ideje implementirane u konkretan program koji služi u poboljšanju anonimnosti na mreži (Tor Project, n.d.).

TOR, kao projekt, nastao je 2002. godine te je služio u osiguravanju sigurne komunikacije unutar američke vojske i vlade. Projekt se može podijeliti u tri generacije: ideje ili prvu (1995. – 2002.), drugu (2002. – 2005.) te treću koja je trenutno aktivna. Program je popularan – u 2021. broji 2,5 milijuna aktivnih izravnih konekcija dnevno. Razlog popularnosti je njegovo jednostavno preuzimanje i uporaba na najpoznatijim platformama dok je korištenje

i traženje usluga putem URL-a otežano zbog 56-oznakovnog *hashiranja* IP-a usluge koje će biti objašnjeno u nastavku.



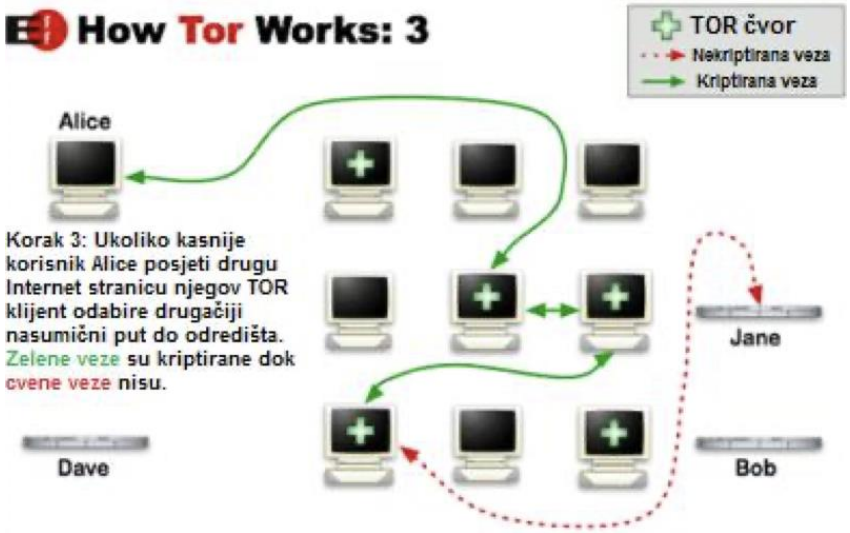
Slika 16. Broj korisnika TOR projekta (2011.-2021.).
Izvor: https://metrics.torproject.org/userstats-relay-country.html?start=2005-06-12&end=2021-09-10&country=all&events=off

4.2.1. NAČIN RADA TOR-a

U nastavku, na slikama 17., 18. i 19. pojednostavljeno su prikazani koraci korištenja TOR-a:

Slika 17. Način rada TOR-a, 1. korak (cis.hr, 2012.).

Slika 18. Način rada TOR-a, 2. korak (cis.hr, 2012.).



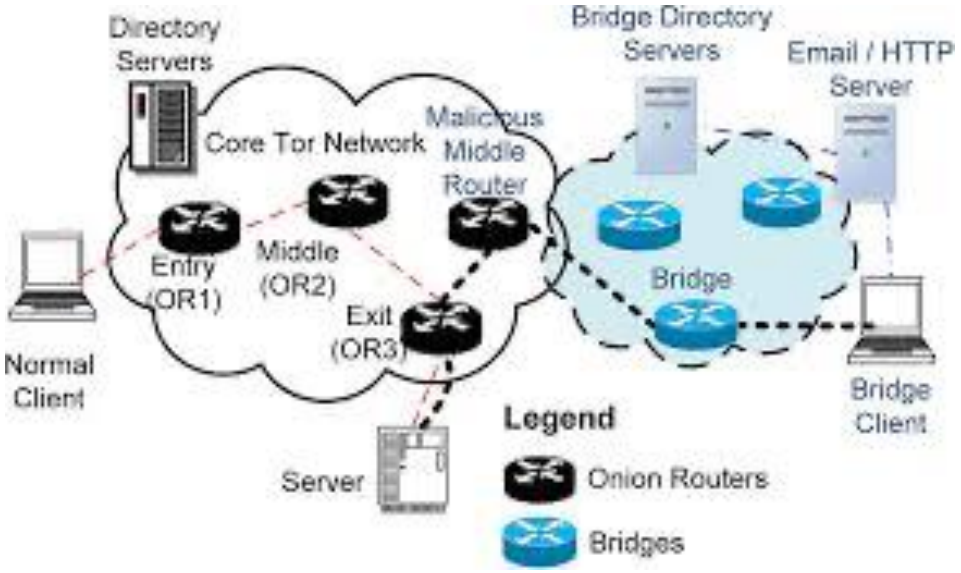
Slika 19. Način rada TOR-a, 3. korak (cis.hr, 2012.).

Nakon određenog vremenskog razdoblja (većinom u desecima minuta) ili nakon što korisnik odabere drugo odredište, stvara se novi lanac kako bi analiza prometa bila onemogućena. Uspoređujući ideju *onion routinga* i implementaciju TOR-a, podudaraju se u osnovnim konceptima, ali zbog problema navedenih u poglavlju 4.1.3., TOR implementira dodatne modifikacije koje rješavaju navedene probleme ideje *onion routinga*.

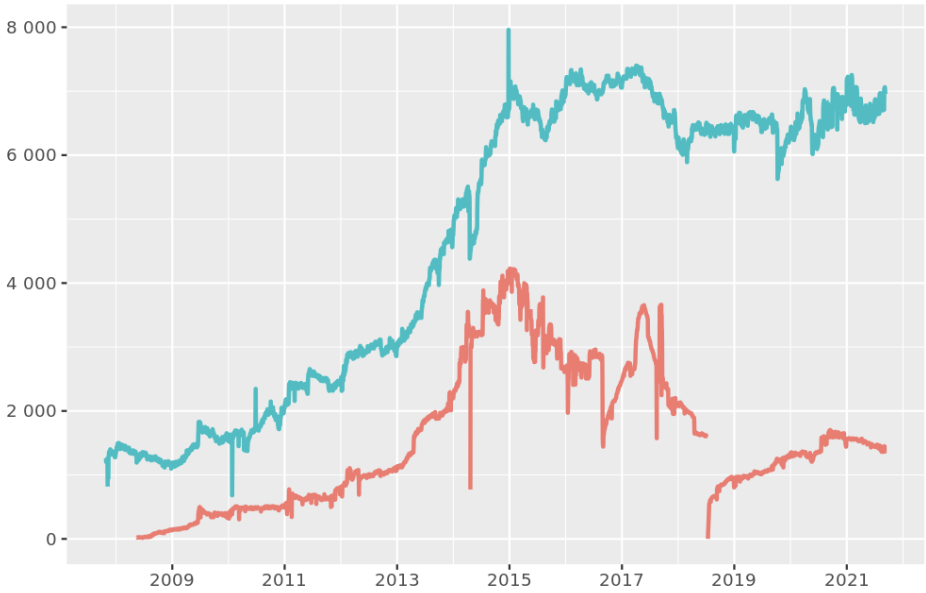
U TOR mreži postoje tri vrste čvorova (Tor Project, n.d.):

- Ne izlazni čvorovi - svi čvorovi koji nisu zadnji čvorovi u lancu. Postoji razlika između neizlaznih čvorova kako mogu biti zaštitni i srednji. Zaštitni čvor je prvi u lancu te postoje određene specifikacije koje mora zadovoljiti, a jedna od njih je da zaštitni čvor ima stabilnu brzinu prijenosa od 2MB/s.
- Izlazni čvorovi – zadnji čvor u lancu koji šalje promet na odredište. Korisnici TOR-a koji se spajaju na različite usluge mogu vidjeti IP adresu zadnjeg čvora umjesto IP adrese korisnika.
- Mostovi su rješenje koje služi za ostvarivanje još veće sigurnosti na TOR mreži. Po specifikaciji mreže sve IP adrese TOR čvorova su javne, ali ukoliko korisnik želi sakriti takve informacije koristit će mostove. Mostovi predstavljaju čvorove koji nisu zapisani u javnoj TOR-ovoj listi čvorova te je pristup i istraga istih otežana. Moguće je otkrivanje mostova ubacivanjem istraživačkog srednjeg čvora koji kada vidi kako mu je podređeni ili nadređeni čvor jedan od čvorova koji nije zapisan u TOR-ovoj listi čvorova, tada će otkriti kako je navedeni čvor most.

Na slici 20. prikazana je izvedba mreže sa svim navedenim vrstama čvorova (Ling, et al., 2015.).



Slika 20. Izvedba TOR mreže sa zaštitnim čvorom ili neizlaznim čvorovima (OR1, OR2), izlaznim (OR3) te mostom (Bridge). Dodatak je istraživački srednji čvor (MMR).
Izvor: https://nymity.ch/sybilhunting/pdf/Ling2015b.pdf

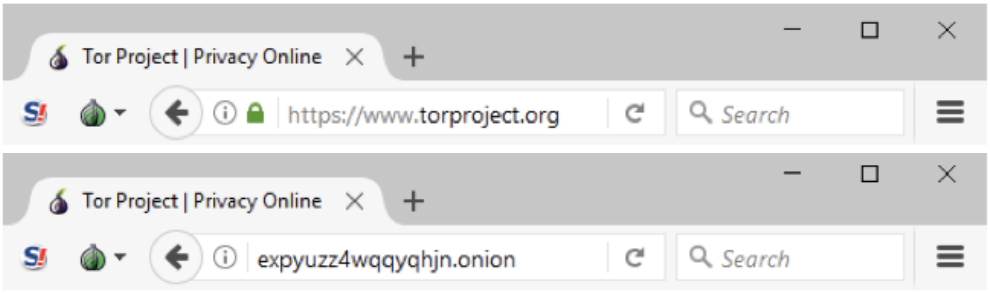


Slika 21. Broj čvorova (plavo) i mostova (crveno) u TOR mreži (2008.-2021.).
Izvor: https://metrics.torproject.org/networksize.html?start=2005-06-12&end=2021-09-10

4.2.2. USLUGE *ONION*

Usluge *onion* su mrežni servisi (stranice) kojima je pristup moguć jedino uz korištenje TOR-a. Ovakve usluge omogućuju sljedeće prednosti u odnosu na *javni web*:

- lokacija te IP adresa usluga je skrivena,
- promet između korisnika TOR-a i *onion* usluga je kriptiran s obje strane (eng. *end-to-end*),
- adrese *onion* usluga su automatski generirane te omogućuju korisnicima da stvaraju svoje *linkove* bez plaćanja domena,
- Nastavak .*onion* omogućuje TOR-u saznanje kako je u procesu spajanje na pravu lokaciju te da komunikacija nije komprimitirana.



Slika 21. Konvencionalna adresa stranice (gore) te adresa onion usluge (dolje).
Izvor: https://nymity.ch/sybilhunting/pdf/Ling2015b.pdf

Onion usluge prepoznatiljive su po svojem sufiksu „*.onion,*" adrese koje se automatski generiraju na javnom ključu prilikom stvaranja usluge. U verziji broj 2, usluge su imale 16-oznakovni nasumični *string* dok u novim verzijama imaju 56-oznakovni nasumični *string*.

Izvješće Sveučilišta Princenton (Winter, et al., 2018.) došlo je do rezultata da su glavni razlozi korištenja *onion* usluga većinom znatiželja ili bez odgovora. Od konkretnih razloga većina koristi *onion* usluge u polju sigurnosti i automatskog kreiranja *linkova*.

4.2.3. NEDOSTACI TOR-A

Najranjiviji dijelovi TOR-a su ulazne i izlazne točke kao i u ideji ovakve tehnike ostvarivanja veće anonimnosti. Napadač može otkriti detalje poruke ukoliko napadne korisnika TOR-a, tj. njegov uređaj gdje više ne ovisi je li poruka kriptirana ili ne.

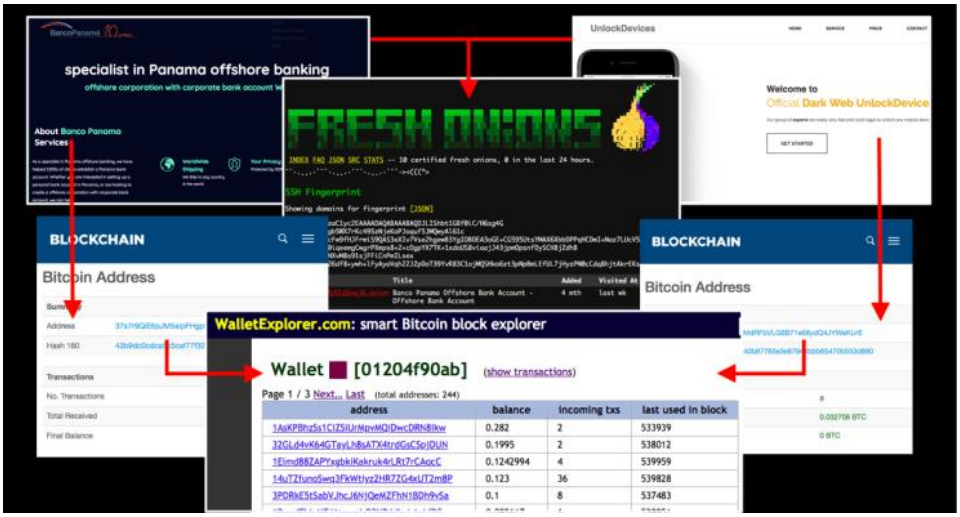
Stalnim širenjem mreže sve je veća potreba za novim ruterima u TOR mreži te je potencijalna opasnost svaki od njih jer analizom jednog, ukoliko je ranjiv, mogu se otkriti vrijedne informacije o mreži kao i otkriti „nevidljive" čvorove (mostove). Jedan od nedostataka je i dovoljno nepažljiv korisnik koji može ostaviti vrijedne podatke na TOR mreži.

Postizanjem novih razina anonimnosti dolazi do zlouporabe anonimnosti. *Onion routing* služi kao podloga za skrivanje zlonamjernih i nelegalnih aktivnosti. Neki od oblika takvih radnji jesu neovlaštena distribucija softvera, autorskih djela i sl., pa sve do krađa, obmana te krajnje neprikladnog sadržaja, gdje je značenje „neprikladnog" preblaga riječ.

Dijelu takvog sadržaja nije moguće pristupiti putem konvencionalnih preglednika, ali ni putem konvencionalnih *linkova*. Za pristup takvim stranicama potrebno je koristiti TOR i poznavati skrivene *„.onion"* usluge. Na posebnim adresama koje služe kao tzv. "liste" usluga mogu se pronaći adrese koje vas vode na najtamniju stranu interneta, *mračni web*.

5. MRAČNI WEB

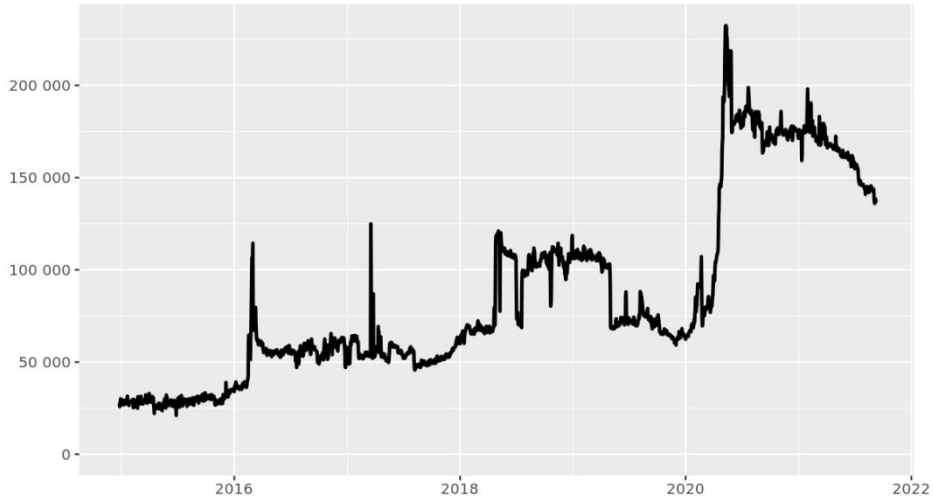
Mračni web svoj je naziv dobio zbog sadržaja koji se na njemu pojavljuje, ali i pristupa koji nije javno svima poznat. *Mračni web* postao je središtem svih nelegalnih aktivnosti na internetu ponajviše zbog anonimnosti koja mu je omogućena.



Slika 22. Izgledi usluga na mračnom webu.

Izvor: https://i2.wp.com/benjaminstrick.com/wp-content/uploads/2020/08/1_KW3mcwk6r1nHDPYU2lO0bA.png?resize=740%2C395&ssl=1

Izgled takvih stranica, tj. skrivenih usluga odstupaju od konvencionalnih stranica. Većinom odražavaju značenje "mračnog". Budući da su to većinom adrese sa prefiksom *.onion,* putem javno dostupnih mjerenja TOR-a dolazi se do podatka kako je broj skrivenih usluga u 2021. godini ispod 150 tisuća.



Slika 23. Broj .onion usluga (2015.-2021.).

Izvor: https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2005-06-13&end=2021-09-11

U nastavku, navedene su najzastupljenije vrste aktivnosti koje se događaju na mračnom webu:

- manipulacija ilegalnim supstancama,
- trgovanje ljudima,
- curenje informacija,
- dječja pornografija,
- preusmjeravanje stranica i krađa,
- prodaja oružja,
- unajmljivanje ubojica,
- nasilan i uznemirujuć sadržaj (Kaur & Randhawa, 2020.).

Važno je navesti kako osim negativnih strana koje nosi, *mračni web* bilježi sve veći rast u pokretanju aktivističkih kampanja te u novinarskim člancima gdje novinari zadržavaju svoj identitet skrivenim (PA Consulting, n.d.).

U istraživanju Gokhalea i Olugbara (2020.) u razdoblju od pet tjedana u 2020. u kojem se računao broj pregleda određenog sadržaja na *dark webu*. Na slici 24. prvi stupac predstavlja sadržaj stranice, drugi stupac predstavlja broj posjeta te treći označava je li stranica neprikladna ili ne.

URL Classification	Hits	Illicit (Y/N)	URL Classification	Hits	Illicit (Y/N)
Social networks	2,208,750	N	Science	139,113	N
Job search	718,900	N	Finance	139,000	N
Web TV	651,326	N	Ringtones	138,320	N
Advertising	567,840	N	News	137,718	N
Web radio	519,586	N	Religion	136,956	N
Update sites	389,474	N	Dating	136,398	N
Porn	285,348	Y	AnonVPN	135,300	N
Spyware	277,695	Y	Podcasts	134,536	N
Sex	180,235	N	Models	133,750	N
Forum	169,024	N	Gamble	133,358	N
Automobile	163,080	N	Recreation	133,342	N
URL shortner	158,928	N	Aggressive	132,990	N
Tracker	157,724	N	Image hosting	132,225	N
Government	157,718	N	Search engines	129,870	N
Alcohol	156,536	N	Politics	129,840	N
Hacking	153,504	Y	Remote control	127,534	N
Radio/TV	151,008	N	Violence	124,440	Y
ISP	150,282	N	Hospitals	124,230	N
Homestyle	148,720	N	Shopping	123,903	N
Music	147,828	N	Education	123,615	N
Webmail	147,318	N	Hobby	122,089	N
Web phones	144,823	N	Library	121,847	N
Warez	144,807	N	Movies	121,555	N
Drugs	143,360	Y	Weapons	118,215	Y
Military	142,740	N	Dynamic	115,107	N
Chat	140,990	N	Total URL hits	11,763,480	
Downloads	140,685	N			

Slika 24. Promet na dark webu (Gokhale & Olugbara, 2020.).

Mračni web postao je plodno tlo za kriptovalute koje su otvorile novi način pranja novca na ilegalnim internetskim marketima. U Siggijevom članku (2020.) predstavljeni su trendovi rasta transakcija na *mračnom webu*. Trgovanje drogom u razdoblju od 2012. do 2015. naraslo je za 1.200% te je 2015. iznosilo 180 milijuna američkih dolara. S druge strane, transakcije u kriptovalutama, ponajviše *bitcoinu* narasle su na 1 milijardu dolara u 2019. godini.

6. ZAKLJUČAK

Pravilnom edukacijom potrebno je uputiti ljude u krivo tumačenje termina koji se koriste u svakodnevnom životu, a vezani su uz internet. *Duboki web* je mjesto u kojemu se događaju nezakonite stvari, ali taj dio je samo maleni dio ukupnog *weba* jer *duboki web* sam čini 90% ukupnog dijela cijelog *weba*. *Duboki web* u većem dijelu slučajeva predstavlja sadržaj kojemu je pristup zabranjen iz sigurnosnih razloga te oni ne moraju nužno biti zlonamjerni. Većinom je to podatkovni sadržaj velikih stranica koje koristimo na *površinskom webu* u obliku baza podataka koje moraju ostati zaštićene kako bi svi naši računi ili repozitoriji na internetu ostali sigurni.

Iako je maleni dio, *mračni dio weba* predstavlja veliki problem u smislu zlouporabe anonimnosti koju je ideja *onion routinga*, ali i implementacija TOR mreže omogućila. *Onion routing* zamišljen je kao protokol koji će ponuditi ljudima sigurnu komunikaciju kroz višestruka kriptiranja, no nažalost ljudi su iskoristili tehničke prednosti koje daje u krive svrhe.

Anonimnost je omogućila stvaranje platforme za mogućnost korištenja ilegalnih trgovina oružja, droge, ljudi i mnogo više od toga. Kroz svoje nedostatke, TOR omogućuje, uz konstantno nadgledanje i zakonske akcije, smanjivanje takvog tipa usluga nije nemoguće jer većina usluga na *mračnom webu* ili su neaktivne ili su zakonski uklonjene. Jedna od prednosti *mračnog* dijela *weba* koja se veže uz anonimnost jest sloboda govora koja ponajviše pomaže novinarima i aktivistima da prenesu svoje ideje bez straha o posljedicama jer smo svjedoci kako je u svijetu sve veća cenzura sadržaja koji treba biti objavljen.

7. IZVORI

- cis.hr, 2012.. *cis.hr: "Onion routing".* [Mrežno]
  Dostupno na: https://www.cis.hr/files/dokumenti/CIS-DOC-2012-09-061.pdf
  [Pokušaj pristupa 10. 9. 2021.].

- Day, J. D. & Zimmermann, H., 1984.. *The OSI reference model,* s.l.: IEEE Xplore.

- Gale Encyclopedia of E-Commerce, 2021.. *Encyclopedia.com: "History of the Internet and World Wide Web (WWW)".* [Online]
  Dostupno na: https://www.encyclopedia.com/economics/encyclopedias-almanacs-transcripts-and-maps/history-internet-and-world-wide-web-www
  [Pokušaj pristupa 10.9.2021.].

- Gokhale, C. & Olugbara, O. O., 2020.. Dark Web Trafc Analysis of Cybersecurity Threats Through South. *SN Computer Science,* 1(273).

- Kaur, S. & Randhawa, S., 2020.. Dark Web: A Web of Crimes. *Wireless Personal Communications,* 112(1).

- Kolb, D., 2020.. *Traversals: "Surface Web is Only the Tip of the Iceberg".* [Mrežno]
  Dostupno na: https://traversals.com/blog/surface-web/
  [Pokušaj pristupa 10.9.2021.].

- Ling, Z. i dr., 2015.. *Tor Bridge Discovery: Extensive Analysis and,* s.l.: IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.

- Mansourian, Y., 2006.. The invisible web: An empirical study of "cognitive invisibility". *Journal of Documentation,* 62(5), str. 584.-596..

- Miniwatts Marketing Group, 2021.. *Internet World Stats: "Internet Growth Statistics - Today's road to e-Commerce and Global Trade Internet Technology Reports".* [Mrežno]
  Dostupno na: https://www.internetworldstats.com/emarketing.htm
  [Pokušaj pristupa 10.9.2021.].

- Navarria, G., 2016.. *The Conversation: How the Internet was born: from the ARPANET to the Internet.* [Mrežno]
  Dostupno na: https://theconversation.com/how-the-internet-was-born-from-the-arpanet-to-the-internet-68072
  [Pokušaj pristupa 10.9.2021.].

- PA Consulting, n.d. *paconsulting.com: "Why the 'dark web' is becoming a cyber security nightmare for businesses".* [Mrežno]
  Dostupno na: https://www.paconsulting.com/insights/why-the-dark-web-is-becoming-a-cyber-security-nightmare-for-businesses/
  [Pokušaj pristupa 10. 9. 2021.].

- Popović, M., 2002.. *kartografija.hr: Prikazi nacionalnih parkova na webu. Diplomski rad, Geodetski fakultet.* [Mrežno]
  Dostupno na: http://www.kartografija.hr/old_hkd/obrazovanje/diplomski/popovic/2.htm
  [Pokušaj pristupa 10.9.2021].

- Pralas, T., 2008.. *CARNET-ov sys.portal.* [Mrežno]
  Dostupno na: https://sysportal.carnet.hr/node/352
  [Pokušaj pristupa 10.9.2021.].

- Reed, M. G., Syverson, P. F. & Goldschlag, D. M., 1997.. *Anonymous Connections and Onion Routing,* Oakland, California: Naval Research Laboratory.

- Sherman, C. B. & Price, G., 2007.. *The Invisible Web: Uncovering Information Sources Search Engines Can't See.* 7. ur. Medford, New Jersey: Information Today.

- Siggia, S., 2020.. *pideeco.be: "How do criminals launder their money using the Dark Web?".* [Mrežno]
  Dostupno na: https://pideeco.be/articles/dark-web-and-money-laundering/
  [Pokušaj pristupa 10. 9. 2021.].

- Sumits, A., 2015.. *Cisco: The History and Future of Internet Traffic.* [Mrežno]
  Dostupno na: https://blogs.cisco.com/sp/the-history-and-future-of-internet-traffic
  [Pokušaj pristupa 10.9.2021.].

- Susuri, A., 2019.. Dark Web and Its Impact in Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications,* 7(3), str. 30.-43..

- Tor Project, n.d. *Tor Project: "Tor: Overview".* [Online]
  Dostupno na: https://2019.www.torproject.org/about/overview.html.en#overview
  [Pokušaj pristupa 10. 9. 2021.].

- Tor Project, n.d. *Tor Project: "Types Of Relays On The Tor Network".* [Mrežno]
  Dostupno na: https://community.torproject.org/relay/types-of-relays/
  [Pokušaj pristupa 10. 9. 2021.].

- Winter, P. i dr., 2018.. *How Do Tor Users Interact With Onion Services?,* Princeton, New Jersey: Princenton University.

8. POPIS SLIKA

9. POPIS TABLICA