Deep web

Bago, Neven

Sveučilište
Sjever

Završni rad br. 494/MM/2016

Deep Web

Neven Bago, 3703/601

Varaždin, studeni 2016. Godine

Sveučilište
Sjever

Multimedija Oblikovanje i Primjena

Završni rad br. 494/MM/2016

Deep Web

Student

Neven Bago , 3703/601

Mentor

doc.dr.sc. Darijo Čerepinko

Varaždin, studeni 2016. godine

Sveučilište Sjever
Sveučilišni centar Varaždin
ma. brigade 3, ma- 42000 Varaždin

Prijava završnog rada

Definiranje teme završnog rada i povjerenstva

ODJEL: Odjel za multimediju, oblikovanje i primjenu

PRISTUPNIK: Neven Bago | MATIČNI BROJ: 3703/601

DATUM: 12.09.2016. | KOLEGIJ: Medijska komunikologija

NASLOV RADA: Deep web

NASLOV RADA NA ENGL. JEZIKU: Deep web

MENTOR: dr.sc. Darijo Čerepinko | ZVANJE: Docent

ČLANOVI POVJERENSTVA:
1. mr.sc. Vladimir Stanisavljević, v.pred. - predsjednik
2. v.pred. Mario Periša, dipl.ing. - član
3. doc.dr.sc. Darijo Čerepinko - mentor
4. pred. Robert Geček, dipl.ing. - zamjenski član
5.

Zadatak završnog rada

BROJ: 494/MM/2016

OPIS:

Deep web je dio Interneta koji je skriven opd javnosti i do kojeg nije moguće doći klasičnim surfanjem i pretraživanjem. Cilj ovog rada je pokazati do koje mjere se Deep Web razvio te koliko je rasprostranjen i sveprisutan. U radu je opisan proces pristupanja Deep Webu pomoću specijalnog programa te se navode njegove mogućnosti i prednosti nad ostalim web pretraživačima. Istražena je valuta BitCoin koja se koristi u online transakcijama zbog mogućnosti kojom pruža anonimnost.

U radu je potrebno:

- Definirati pojmove vezane uz Deep web
- Definirati pojmove vezane uz TOR
- Definirati pojmove uz BitCoin
- Napraviti studije slučaja spomenutih pojmova
- Dati zaključak o Deep webu

ZADATAK URUČEN: 22.09.2016. | POTPIS MENTORA

Sažetak

Završnom radu „Deep Web“ je cilj da se u osnovi nauči što je on te koliko je rasprostranjen. Korištenjem programa TOR pristupa se „sakrivenom“ dijelu interneta poznatom kao Deep Web. U radu je opisan proces pristupanja Deep Webu pomoću spomenutog programa. Navodi sve njegove mogućnosti i prednosti nad ostalim web pretraživačima. Istražena je valuta BitCoin koja se koristi u online transakcijama zbog mogućnosti kojom pruža anonimnost.

Cilj ovog rada je pokazati do koje mjere se Deep Web razvio te koliko je rasprostranjen i sveprisutan, a da toga nismo ni svjesni.

Prikazan je put razvoja Dark Weba gdje se spominje njegova najpoznatija online tržnica Silk Road koja je zaslužna za porast popularnosti i cijene BitCoina. Silk Road je ujedno bio predmetom jedne od najvećih akcija uhićenja kada je među mnogobrojnim korisnicima Deep Weba uhićen i osnivač Silk Roada, Ross Ulbricht pod nazivom Dread Pirate Robert.

Spomenuti Dark Web je mjesto na kojem je gotovo sav sadržaj ilegalan. Na njemu se odvijaju špijunaže, promatranje servera, razne usluge, preprodaje ogromnih količina droga, prodaja seksualnog roblja pa čak i stranice povezane sa pedofilijom.

Ključne riječi :
Deep Web, TOR, BitCoin, Dark Web

Kratice

TOR – The Onion Router

DDoS-Distribited Denial of Service

ICANN - Internet Corporation for Assigned Names and Numbers

VPN -Virtual Private Network

MIT- Massachusetts Institute of Technology

Summary

The end goal of the final paper „Deep Web“ is to basically learn what Deep Web is and how widespread is it. Using the program called TOR we access the „hidden“ part of the internet known as Deep Web. The paper describes the process of accessing theDeep Web using the program mentioned before. We listed all of its features and advantages over other web browsers. We also investigated the value of BitCoin which is used in online transactions because of its anonymity.

The aim of this paper is to show the extent to which Deep Web developed and how widespread and omnipresent it is, without us even knowing that.

We showed the development of Dark Webwhich mention his largest online market Silk Road which is responsible for the increase in popularity and the price of BitCoin. Silk Road was also a subject of one of the largest arrests when many users of the Deep Web were arrested and among them was the founder of the Silk Road, Ross Ulbricht also known as Dread Pirate Robert.

The mentioned Dark Web is a place where almost all of the content is illegal. Some of the illegal actions that take place on the Dark Web are: espionage, server surveillance, various illegal services, resales of enormus quantities of drugs,sellingsex slavesand even websites linked to pedophilia.

Keywords :

Deep Web, TOR, BitCoin, Dark Web

Abbreviations

TOR – The Onion Router

DDoS-Distribited Denial of Service

ICANN - Internet Corporation for Assigned Names and Numbers

VPN -Virtual Private Network

MIT- Massachusetts Institute of Technology

Sadržaj

1. Uvod 1
2. Podjela Interneta 2
2.1 Deep Web 3
2.2 Dark Web 4
2.3 Borba protiv nevidljivog 6
2.4 Dobar Dark Web 9
2.5 GNU Dark Web 10
2.6 Silk Road 11
2.7 Arhive foruma Silk Roada 14
3. Pristup preko TOR-a 15
3.1 Povijest TOR-a 15
3.2Preuzimanje i prvo pokretanje TOR-a 16
3.3.Kako radi TOR 22
4. BitCoin 23
4.1 Karakteristike 24
4.2 Utvrđivanje cijene Bitcoina 25
5. Istraživanja o Deep Webu 26
6. Zaključak 28
Reference 30

1. Uvod

Za izvedbuovog završnog rada bilo je potrebno istražiti Deep Web: što je, kako mu se pristupa i kako se koristi.Većina ljudi koja se koristi Internetom zna kako pristupiti Googlu, na kojem, uostalom, mogu naći sve informacije koje ih zanimaju. Deep Webu pristupna relativno mala skupina ljudi. Sam pristup je otežan i stranice nije moguće dohvatiti preko Googlea. Deep Web je za potrebe ovog rada istražen pristupom Googla i TORa. Opisano je kako se kupuje pomoću njega, postaje anonimnim te kako izbjeći probleme koje sadržaj ovog dijela Interneta može uzrokovati.

Deep Web je sav sakriveni dio Interneta. Vidljiv Internet je onaj koji je moguće otvoriti Internet pretraživačem i pronaći preko Googla, što znači da je određeni sadržaj indeksirala bilo koja Internet tražilica poput Googla, Yahooa ili Binga.

Po najjednostavnijoj definiciji, Deep Web je sav onaj web čiji sadržaj nije vidljiv većini korisnika i kojemu je pristup otežan, a čiji su korisnici anonimni.

S obzirom na prirodu većine sadržaja Deep Weba, NSA i FBI u organizaciji vlade SAD-a pokušavaju otkriti identitet korisnika. To nije lak zadatak, uzevši u obzir postavke privatnosti i gotovo stopostotnu anonimnost većine korisnika. Valuta kojom se koriste je anonimna i nije je moguće pratiti, a IP adresa je varijabilna.

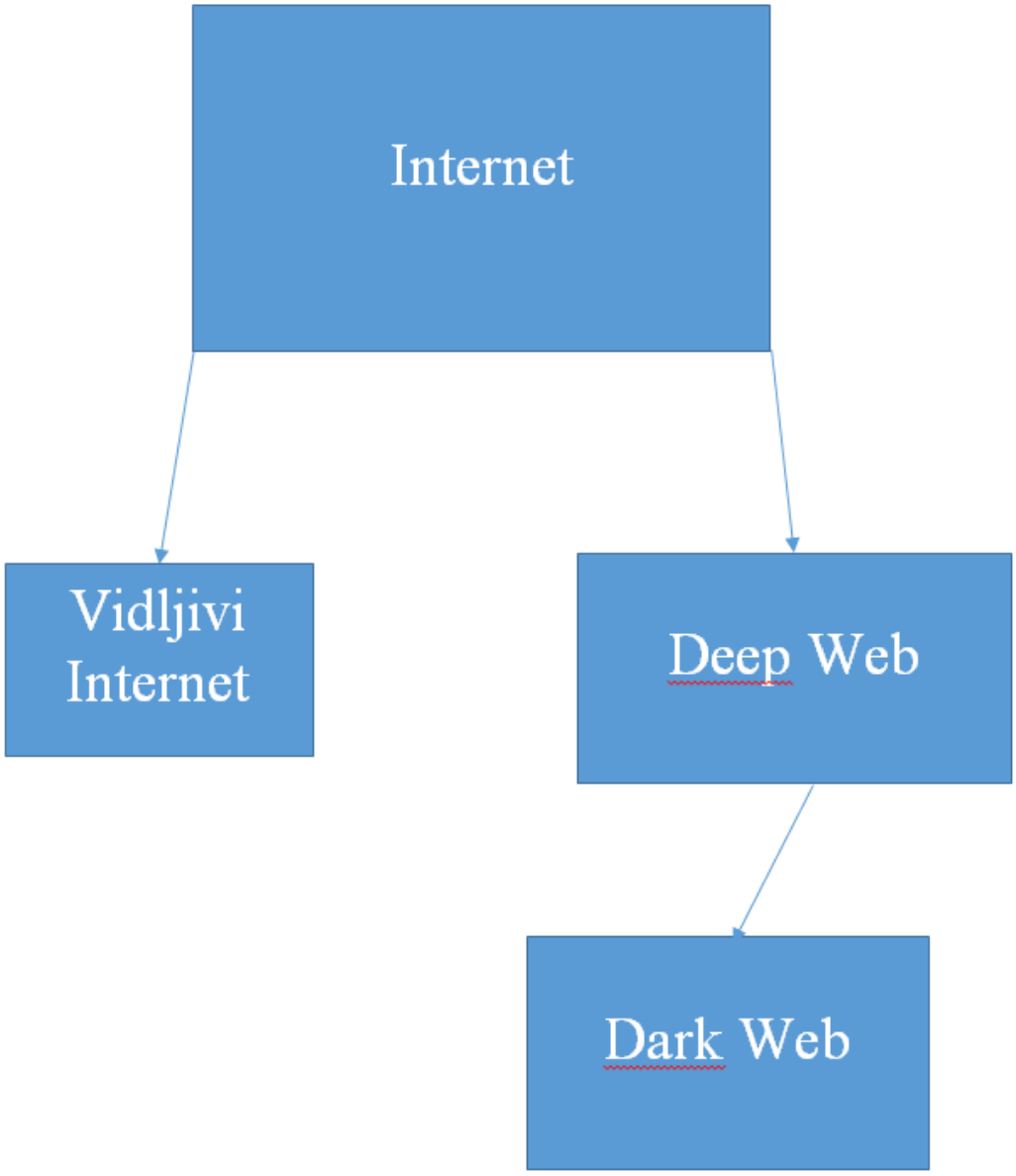
Podaci Deep Weba se sastoje od najobičnijih privatnih web stranica, ogromnih tržnica, privatnih oglasa za usluge, prodaja ukradenih stvari, baza podataka gotovo svih banaka pa sve do baza svih torrenta. Pristup je moguć preko svih web browsera, uz uvjet da se na kraj URL adrese stavi “.to „ no to ne štiti od mogućih prismotra. TOR dodaje dodatan sloj privatnosti čime se korisniku olakšava pretraživanje Deep Weba. Za dodatnu enkripciju preporučuje se korištenje Linux Tailsa.

Osim Deep Weba postoji i Dark Web, koji se smatra strogo ilegalnim zbog svojeg sadržaja. Na Dark Webu se isključivo vrši preprodaja droge, oružja, ukradenih tehnoloških sredstavazatim dječja pornografija pa čak i Red Room. Sav materijal Deep i Dark Weba se plaća s BitCoin-om zbog njegove jako dobre zaštite privatnosti korisnika. Tokom pojave Deep Weba pokušala se ustanoviti njegova veličina, no nikad se nije moglo doći do točne veličine.

2. Podjela Interneta

Podjelu Interneta moguće je kategorizirati u dvije osnovne grupe. Prva je „Visible Web“ gdje je sav sadržaj kojem možemo pristupiti pomoću bilo kojeg Internet pretraživača. Druga grupa je „Deep Web“. U toj grupi se nalazi podskupina pod nazivom „Dark Web“.

Prva grupa Visible Web je nastala još davne 1983. godine kada je ARPANET pridobio TCP/IP protokol. Današnji Internet je postao prepoznatljiv još 1990. kada je računalni znanstvenik Tim Berners-Lee napravio World Wide Web. [16]



Slika 1. Podjela Interneta

2.1 Deep Web

Deep Web nastao je 1994. godine tijekom koje je bio poznat kao „Hidden Web“. Tek 2001. godine je dobio naziv Deep Web. Njegovo glavno svojstvo je raširenost informacija. Dok neke Internet tražilice poput Googla neće pronaći tražene rezulate, tražilice na Deep Webu imaju veći obujam potražnje podataka te imaju veće šanse za pronaći željeni upit.[17]

Deep Web je osnovni alat koji služi novinarima za pristupodređenim informacijama koje nije moguće naći preko Googla. On također služi za sigurnukomunikaciju između policije, a ponajviše između obavještajnih službi, uključujući i banke. Od svih korisnika Interneta, samo 1% njih koristi Deep Web za pretragu informacija. Računi svih banaka su pohranjeni na Deep Webu uz nezamislivo dobru zaštitu podataka. [1]

Osim svih legalnih potraživanja na Deep Webu, postoje ljudi koji koriste Deep Web za sigurno izvršavanje kriminalnih radnji, poput prodaje droge i oružja, distribucije dječje pornografije, unajmljivanja ubojica pa čak i kupnju ukradenih PayPal računa, mobitela i računala. Korisnici Deep Weba s namjerom kupnje ili prodaje koriste posebnu valutu, BitCoin. No tu počinje Dark Web.

2.2 Dark Web

Dark Web je najdublji dio Deep Weba. Često se naziva i dramatičnim zbog svoje prirode. No on je ipak veći i drugačiji od svih ilegalnih aktivnosti na njemu. Ona ista tehnologija koja omogućuje rad u sjeni raznih online tržnica, istovremeno štiti ljude cijelog svijeta i njihove svakodnevne potražnje od nadzora na Internetu. [12]

Većina ljudi smatra Internet medijem za komunikaciju, istovremeno ne znajući da tek „plove po površini". TOR se može koristiti i za pristup stranicama izvan Deep Weba, ali server mora biti posebno adresiran da se može dohvatiti unutar TOR-a. To se naziva skrivenim servisima. Kad se misli na skrivene servise, misli se na Dark Web i njegove stranice. Postoje i drugi servisi za sakrivanje aktivnosti na Internetu, ali TOR je najpoznatiji i najrazvijeniji.[12]

„Prije nekoliko godina, kad se pokušavalo pretraživati Internet pomoću TOR-a, bilo je to jako sporo i jako bolno iskustvo." riječi su istraživača Stefana Tanasea, zaposlenika Kasperskya.[12]
Digitalni sigurnosni stručnjaci poput Stefana i njegovog suradnika iz Moskve Sergeya Lozhkina često imaju pune ruke posla jer baš iz New Yorka i Moskve dolazi najviše spamova, malwarea i cyber napada. Obojica imaju jedinstvenu perspektivu na sakriveni eko sistem Dark Weba. Dok površinski Web sadrži sistem indeksiranja, Dark Web ne sadrži nikakvu kartu konekcija na Dark Webu. Stoga su odlučili samostalno napraviti neku listu stranica.

„Započeli smo s listom poznatijih sakrivenih stranica unutar TOR mreže te smo koristili Web Crawler, da pristupimo tim stranicama i tražili poveznice prema drugim stranicama.", izjava je Stefana Tanasea [12], koji opisuje proces rada Web Crawlera na koji Google radi kada indeksira stranice. Iako je broj sakrivenih servisa na TOR-u, u usporedbi sa Internetom u cjelini, relativno mali, znanstvenici izjavljuju da Dark Web ostaje misterija čak i nakon istraživanja.

Prema Lozhkinu :„Postoji veliki broj stranica koje se svakodnevno gase i nisu dostupne mjesecima ili tjednima. U sljedećih nekoliko sati, stranice sa istim sadržajem dostupne su na potpuno drugim adresama". [12]

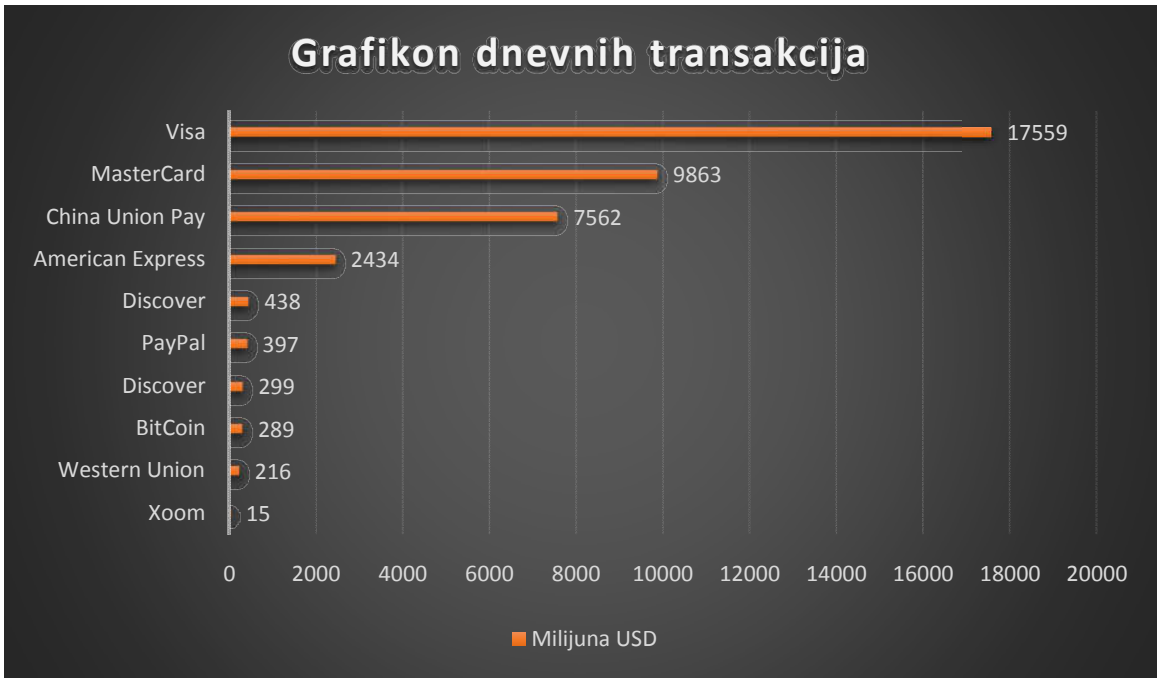
Danas postoji i službena TOR verzija za Android uređaje. Koristi sličan način pretraživanja koji su koristili i tehničari za Kaspersky, dakle već postoji tražilica za Dark i Deep Web.

Ovako većina ljudi zamišlja Dark Web : elektronička tržnica gdje je sve dostupno. Znanstvenici to potvrđuju, ali istovremeno dodaju da je sve još puno gore. Sve je dostupno preko sakrivenih stranica, dohvatljivima samo preko TOR-a. Droge, oružja te rogovi nosoroga su na prodaju, ali i dalje zahtijevaju fizičku interakciju za razmjenu robe.[12]

Dark Web je bez ikakvog ispitivanja opasniji kad dolazi do lake distribucije ilegalnog digitalnog materijala, primjerice dječje pornografije. U 2011. godini Dark Web stranica „Lolita City“, koja distribuira dječju pornografiju, bila je meta Anonymousa. Tada su je isključili i pustili u javnost informacije o njezinim pokroviteljima. U to vrijeme bilo je prijavljeno da stranica sadrži preko 100 GB dječje pornografije. Uhitili su Erica Eiona Marquesa, operatora TOR hosting servisa „Freedom Hosting“koji je davao podršku stranici Lolita City. [12] [18]

2.3 Borba protiv nevidljivog

Andrew Conway koji radi za Cloudmark, antispam tvrtku koja je povezana sa preko 120 važnijih pružatelja komunikacija zna kako djeluju kriminalne mreže te kako novac putuje između tih skupina. Sve se svodi na BitCoin i Silk Road. [12] Porast BitCoina je ponajviše povezan sa SilkRoadom. Kupovina unutar svih kategorija bila je moguća i preko PayPala, ali problem je bio u sigurnosti valute. PayPal je siguran, ali nije anoniman poput BitCoina. PayPal je, kao i BitCoin, namijenjen potrošačima, ali se također fokusira na prodavače. [13]



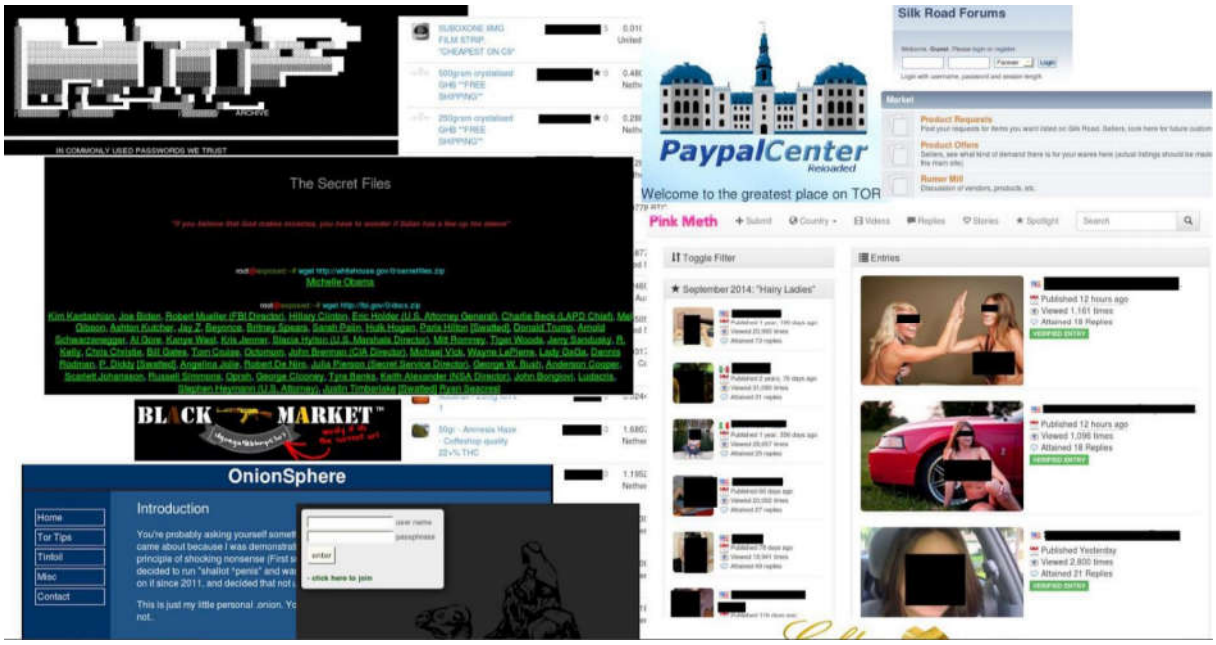
Slika 2. Usporedba dnevnih transakcija među valutama (prosinac 2013) [14]

Prema Lozhkinu : „Cijeli Deep Web sastoji se od web stranica i svaka stranica može imati slabosti.Ako snage zakona pronađu slabost mogu je lako iskoristiti da uđu u server. Ako dobiju pristup serveru, lako je identificirati lokaciju servera.“[12] U slučaju Silk Roada, mala greška igra veliku ulogu. Tanase je izjavio da je operater Silk Roada upravljao serverom iz Internet Cafea te se spajaodirektno na server, a ne preko TOR-a. Ironično, takve male greške koje kriminalci često rade pomažu vlastima da pronađu njihove slabosti u napadima na tvrtke i pojedince. Kako god bilo, snage zakona identificiraju server na kojem se nalaze stranice sa ilegalnim sadržajem te za cilj imaju preuzeti kontrolu nad tim serverom. Tanase je izjavio „Obično zatraže nalog za promatranje servera i pokušavaju izvući informacije iz servera kada

je aktivan što omogućava praćenje kriminalaca.“[12] On pretpostavlja da snage zakona i same prodaju ilegalne stvari kako bi namamile potrošače.

Naravno, postoji i više nego dovoljno načina napada da se izlože strojevi koji održavaju sakrivene webstranice unutar TOR-a. Tanase kaže da ako postoji samo jedan entitet koji je u kontroli obujma između TOR-ovih čvorova, može se pratiti cijeli Internet promet u cijelom sistemu. Naravno, to ne može napraviti pojedinac ili cijela agencija, već sve ovisi o čvorovima. Što ih je više u kontroli, više se može saznati. [12]

Tanase i Lozhkin opisuju još odvažniju shemu lociranja svih sakrivenih procesa na TOR-u. Trebalo bi odabrati sve IP adrese u određenom dometu, primjerice cijele države i postepeno ih preplaviti sa lažnim zahtjevima kao što je DDoS napad . Tijekom tog napada, napadači bi pažljivo motrili na status sakrivenih TOR stranica. Kada bi vidjeli da je stranica dolje ili prilikom primjetnog povećanja prometa na stranici, znali bi da su napravili dobar udarac na grupu IP adresa. Zato bi napadači trebali savjet u vezi lokacije servera da započnu napad. To su informacije koje mogu pribaviti tajni agenti, ili se mogu pronaći „stalkanjem“ sakrivenih foruma gdje Deep Web operateri raspravljaju. Takav napad zahtjeva veliku količinu resursa i veliku volju da se upadne unutar TOR-a. Taj način napada bi samo privremeno ugasio TOR-ove usluge. Kad bi se dogodio veliki DDoS napad, Conwaysmatra[12] da bi se i Deep Web mogao ugasiti za stalno.



Slika 3. Razni sakriveni servisi Dark Weba [12]

Gotovo svakodnevno provodi se 1200 DDoS napada. Jedan napad na IP adrese sa vidljivog Weba bez upotrebe TOR-a limitirao bi mogućnost prolaženja prometa kroz čvorove i učinio bi TOR mrežu beskorisnom.

Čak se i TOR prigušio na budućnost svojih servisa. Nakon što je Vlada SAD-a oduzela i ugasila preko 400 web stranica u samo jednoj operaciji (Onymus)[12], pojavio se članak na službenoj stranici TOR-a koji je sadržavao sljedeće: „Na bilo koji način, iznenađujuće je da su sakriveni servisi preživjeli i ovoliko dugo. Pažnja koju su dobivali je minimalna uspoređujući sa njihovom socijalnom vrijednosti i uspoređujući sa količinom odlučnosti svojih protivnika.“

2.4 Dobar Dark Web

Protivnici Dark Weba najčešće se identificiraju kao snage zakona, ali ne ulaze uvijek u posao sa zatvaranjem krugova droga ili proganjanjem trgovaca ljudskim robljem. Ti špijuni koji rade za državu svojom snagom povećavaju kapacitet elektroničkog izražaja. To je zbog toga jer su pod istom zaštitom TOR-a kao i ostali kriminalci koji se koriste njime. Iako su zakoni u SAD-u do nedavno opustošili TOR-ove sakrivene servise, razne vladine agencije nastavljaju financirati TOR. Vlada SAD-a još uvijek,bez ikakve sumnje, nalazi korist u TOR-u i nastavlja poticati zadatak promocije slobode govora iz drugih zemalja.

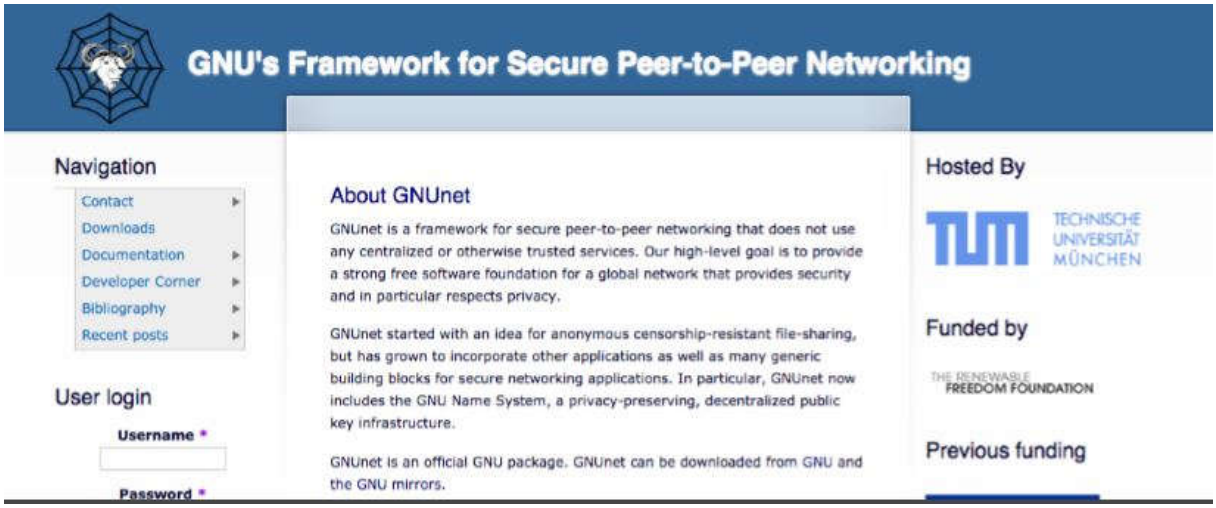
2.5 GNU Dark Web

2014. godina je nesumnjivo bila zastrašujuća za digitalnu sigurnost. Briga oko toga da NSA mjesecima prati sve građane SAD-a zatim masovne povrede privatnosti koje su šokirale svijet i argumentiranje svega preko Interneta dovelo je do narušavanja kongresa SAD-a.[12]

To su problemi inženjerstva, a ne politike, kako ih se klasificiralo i ti problemi traže sigurnosne stručnjake. Jedan od njih je Christian Grothoff. On se nada da će sve ispraviti sa GNUnet-om, kojeg je pokrenuo još 2001. godine kao besplatan software. Pokušavao je napraviti sigurnu P2P mrežu, poput TOR-a. Ona je dizajnirana sa sigurnosnim i anonimnim postavkama u planu, ali za razliku od TOR-a, ona ne zahtjeva arhitekturu Interneta takvog kakav je poznat većini ljudi (TCP/IP).

TCP/IP dopušta svima istraživanje nečije povijesti prometa na Webu, a oslanja se na centralni autoritet poput ICANN koji upravlja DNS-om. Grothoff je izjavio: „Objasnite mi, zašto IP paket mora sadržavati izvorni IP u sebi? Kako bismo ga preusmjerili, potrebno nam je samo odredište. U TOR-u taj paket samo skače okolo. Možemo napraviti novi protokol gdje je taj podatak već enkriptiran.“

GNUnet je mreža na kojoj pojedinci koriste privatnost koja štiti njihovo ime, umjesto DNS-a za koji ne treba centralni autoritet. Prema svojoj prirodi trebao bi se štititi sam po sebi od promatranja za koji je bila optužena NSA. [12]



Slika 4. GNUnet web stranica [15]

2.6 Silk Road

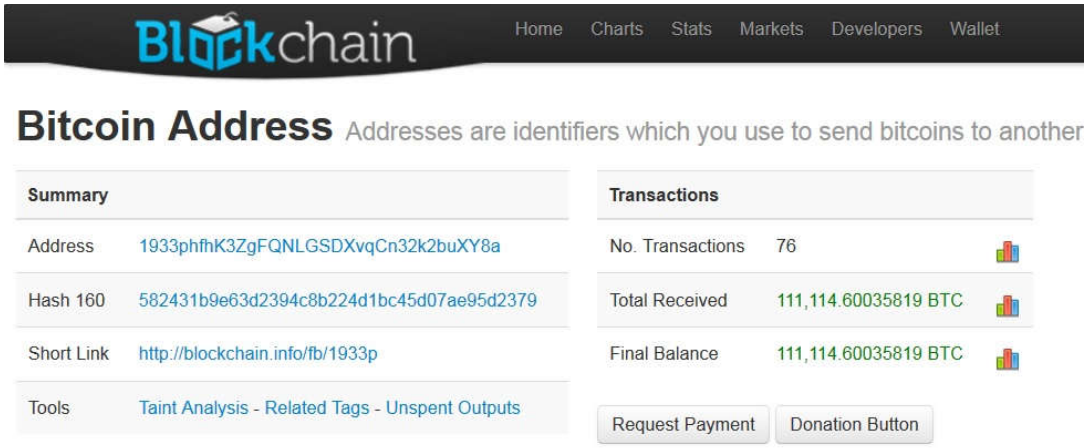
Silk Road je Dark Web stranica slična e-Bayu. Glavna je razlika u tome što je ova stranica bila sakrivena i bilo je nemogućepretraživati sadržaj bez registracije i bez valjanog BitCoin računa. Naziv je dobila po povijesnoj ruti koja je povezivala Kinu i Sredozemno more. Na Dark Webu „Dread Pirate Roberts“ (DPR) pokretač stranice, najpoznatije masivnoj prodaji droge. Naravno, sve je to bilo ilegalno, no budući da se odvijalo preko TOR-a, bilo je anonimno i sigurno za pretraživanje. Silk Road je osnovan u veljači 2011. godine i nije svatko mogao postaviti svoju aukciju. Iz sigurnosnih razloga, za postavljanje aukcija prvo se morao kupiti isti račun. Kasnije je bila postavljena stalna cijena za svakog tko je htio postati prodavač. U listopadu 2013. FBI je ugasio Silk Road i uhitio Rossa Williama Ulbrichta pod optužbama da je upravo on bio DPR.

Nakon zatvaranja Silk Roada, 6. studenog 2013.godine, otvorena je nova stranica Silk Road 2.0, koju su vodili bivši administratori Silk Roada. Ona je također nakon nekog vremena bila ugašena, a voditelji stranice bili su uhićeni.

Ulbricht osuđen je na temelju 7 optužbi, koje su povezane sa Silk Roadom i zatvoren doživotno bez mogućnosti pomilovanja. Za neke optužbe još čeka suđenje.[8]

U siječnju 2015. otvara se stranica "Silk Road Reloaded", koja podržava više načina plaćanja.

Pošto je FBI ugasio server, njihova vlada postala je novi vlasnik svih BitCoin računa koje su zaplijenili s njima. Među svim računima nađen je račun od DPR-a koji je sadržavao 111,000 BitCoina, koji su u to vrijeme vrijedili 17,000,000 $. [11]



Slika 5. BitCoin račun pronađen na SilkRoadu

Silk Road market većinom je služio za prodaju droga. Osim droga, prodavane su lažne osobne karte, odjeća, umjetnine, knjige, suveniri, oprema za računala, digitalna roba, elektronika, vatrometi, hrana, oprema za dom i vrt, nakit, oprema za laboratorij, liječnička oprema, novac, usluge, sportska roba, oružja, pornografija i još mnogo toga.

Forgeries(15)
Fake IDs(8)
Apparel(1)
Art(26)
Books(186)
Collectibles(1)
Computer equipment(5)
Digital goods(100)
Drug paraphernalia(33)
Drugs(2150)
Electronics(10)
Fireworks(1)
Food(1)
Home & Garden(2)
Jewelry(2)
Lab Supplies(9)
Medical(4)
Money(93)
Services(47)
Sporting goods(1)
Weaponry(19)
XXX(48)

sort by bestselling go

title	price	seller	ship from	
Ultimate Fake ID Guide / Templates / Sources / kit	฿0.27	warweed(99)	undeclared	add to cart
ATM scam keeping your stores machines safe	฿0.49	warweed(99)	undeclared	add to cart
Barcode Manipulation scam keeping your store safe	฿0.49	warweed(99)	undeclared	add to cart
Beat the Online Casinos [FREE FEB 4th-5th!]	฿0.00	RickyRango(97)	undeclared	add to cart
Scannable Fake ID	฿22.14	KingOfClubs(100)	undeclared	add to cart
Driver's License & Health Card Combo	฿42.00	KingOfClubs(100)	undeclared	add to cart
Student ID Card	฿13.50	KingOfClubs(100)	undeclared	add to cart
NJ ID UV/Scannable/Holo	฿16.86	legionx	undeclared	add to cart
custom for Dmitrii	฿20.24	legionx	undeclared	add to cart
UK Drivers license UV and Hologram	฿50.59	googleyed(100)	United Kingdom	add to cart
Texas Drivers License (Holograms + Scannable)	฿24.00	KingOfClubs(100)	undeclared	add to cart
Alberta Drivers License (Hologram + Scannable)	฿24.00	KingOfClubs(100)	undeclared	add to cart
PM us with your requested id or drivers license !!	฿0.01	idworldwide	undeclared	add to cart
Custom for John	฿84.32	legionx	undeclared	add to cart
Ontario Drivers License (Holo, Raised LTR, Scans)	฿24.00	KingOfClubs(100)	undeclared	add to cart

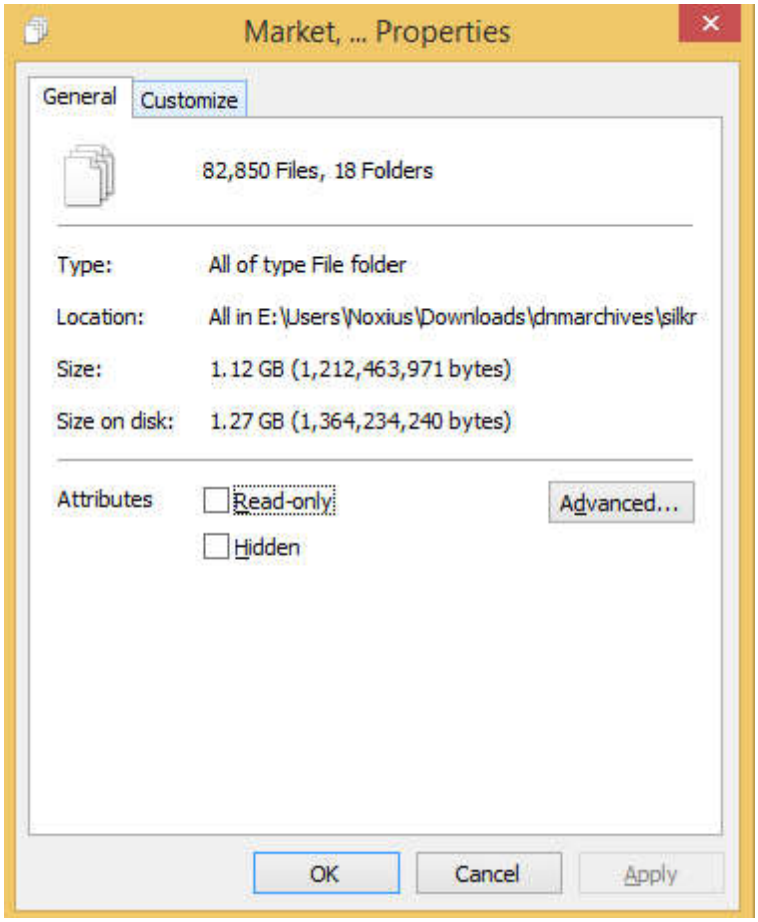
Slika 6. Silk Road market

Tijekom jednog dana bilo je obavljeno oko 100 transakcija koje su imale prosječnu vrijednost od 150$. Kako je Silk Road bio održavan 2 godine, zaradio je samo od održavanja stranice preko 10,950,000 $. Razvoj Silk Roada najviše je utjecao na BitCoin, kojem je u tomrazdoblju porasla cijena.[10]

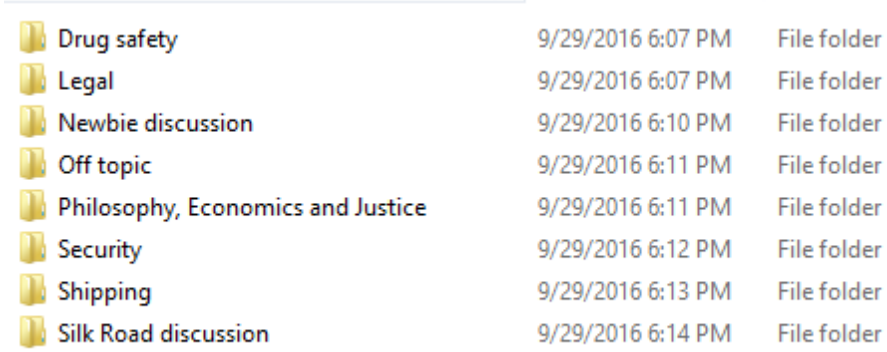
Slika 7. Obavijest na Silk Roadu 2.0 nakon gašenja stranice

2.7 Arhive foruma Silk Roada

Preko izvora [19] pristupili smo gotovo svim podacima koji se mogu naći u najvećim Dark Web tržnicama koje uključuju Outlawmarket, Agora, Nucleus, Silkroad2, Evolution,Cryptomarket, Blackbankmarket,Armory i još mnoge druge (sveukupno ih je 87). Svi podaci, kada se izdvoje veličine su 1.6 TB. No zadržali smo se samo na Silk Roadu. Sama Silk Road arhiva velika je 1.12 GB. Arhiva sveukupno sadrži 82,850 tema koje su bile aktualne .



Slika 8. Postavke datoteke SilkRoad Forum arhive



Slika 9.Arhiva foruma

3. Pristup preko TOR-a

3.1 Povijest TOR-a

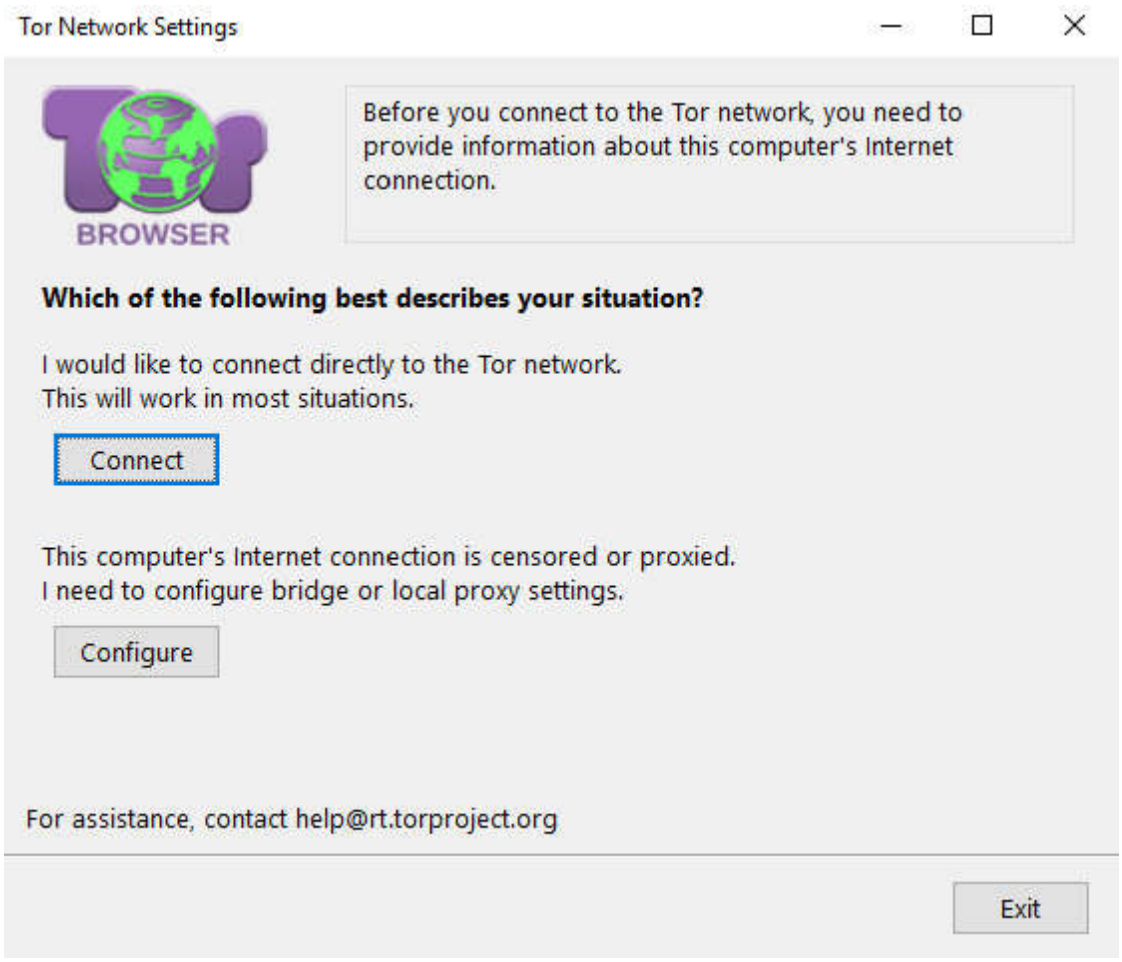
Kako bi pristupila Deep Webu, za početak osoba mora biti upoznata s TOR-om.TORje web pretraživač napravljen s ciljem da ne ostavlja nikakve tragove pretraživanja isto tako pouzdan je za brisanje tragova i lokacija s kojih se preko njega pristupalo.

Za nastanak samog programa zaslužni su informatički stručnjaci Michael G. Reed i David Goldschlag i matematičar Paul Syverson.Prvobitna svrha ovog programa bila jezaštita podataka obavještajnih agencija te omogućavanje sigurnekomunikacije. Tijekom 1997. godine cijeli projekt preuzela je agencija DARPA (Defencese Advanced Research Project Agency) koja ga tada nastavlja razvijati. [2]

Prvu verziju programa su 2002. godinerazvijali Paul Syverson, Roger Dingledine i Nick Mathewson. 2004. godine predstavljaju drugu verziju programa na USENIX okupljanju iz područja sigurnosti na Internetu (Unix User Group). Iste godine pušten je kod programa kao besplatni program koji financiravlada Sjedinjenih Američkih Država.

3.2 Preuzimanje i prvo pokretanje TOR-a

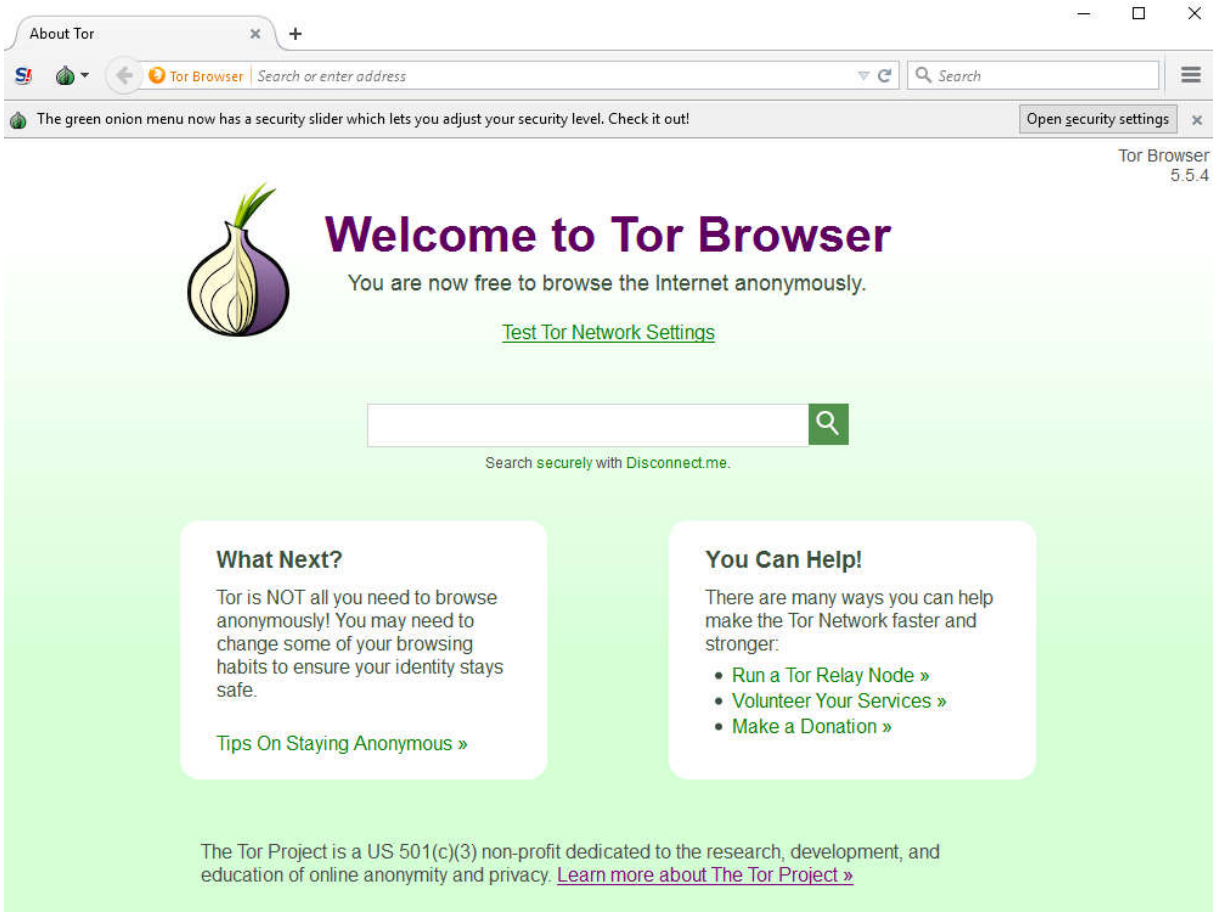
Za početak istraživanja Deep Weba potrebno je računalu omogućiti pristup istom. Prvo je potrebno preuzeti TOR. Veličina programa je 41 MB, a on pruža anonimnost na webu. Nakon preuzimanja i instalacije programa, TOR se pokreće samostalno. Kod prvog pokretanjaponuđeno je automatsko povezivanje na proxy server. Slika 10 prikazuje korak konfiguracije proxy servera, ukoliko je taj korak nužan.



Slika 10. Prvo konfiguriranje proxy servera

Proxy server je korisnikova„lažna“ lokacija koju koristi u jednom spajanju na Internet. Ako se, dakle, spoji na proxy server koji je lociran u Kini, tijekom provjere IP adrese bit će prikazano da je njegovo računalo u Kini. Također, mogu se koristiti VPN-ovi , koji imaju istu svrhu.

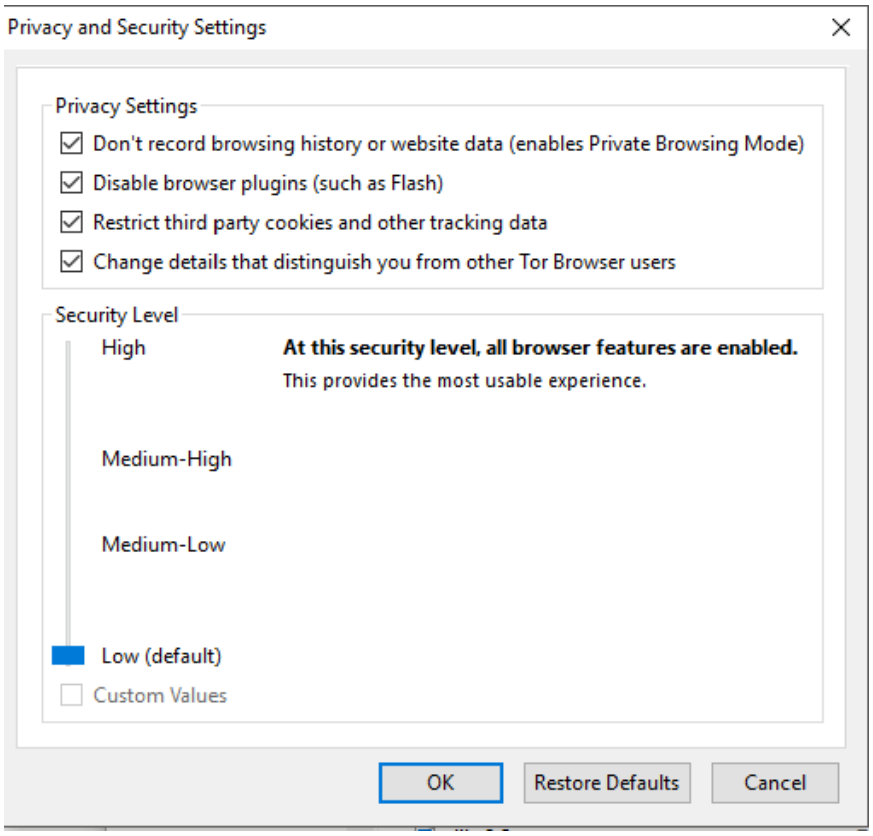
TOR je, dakle, izuzetno siguran za anonimno surfanje Internetom, ali svejedno postoje neke mane. Slika 11 prikazuje početni zaslon TOR pretraživača,na kojemuje vidljivo upozorenje kojepojašnjavakako osigurati anonimnost.



Slika 11. Početni zaslon Tor Browsera

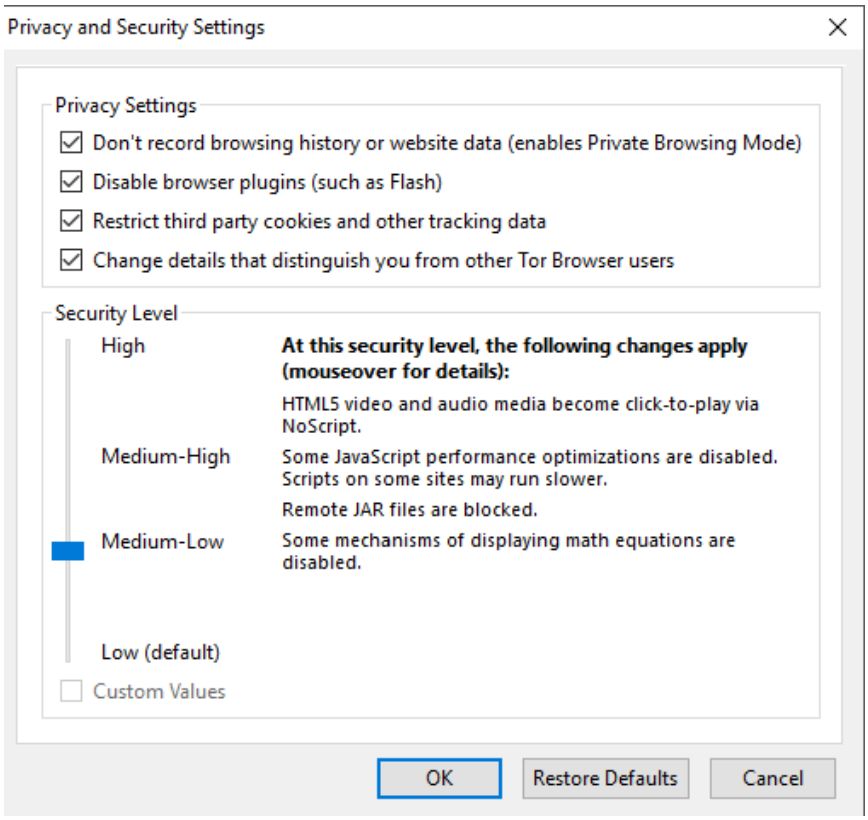
Ostali načini za pokrivanje nedostataka podrazumijevaju korištenje dodatne zaštite poput Linux-ovog OS-a Tails. Tails je besplatna Linuxova inačica koja sadrži u sebi alate za sigurno pretraživanje weba tako da sva Internet povezivanja preko njega se mogu obavljati jedino preko TOR-a, bez ikakvih tragova uz dodatne programe za zaštitu datoteka i e-maila pomoću enkripcije.

Nakon otvaranja postavki privatnosti i zaštite vidljive su 4 opcije koje se mogu uključiti.

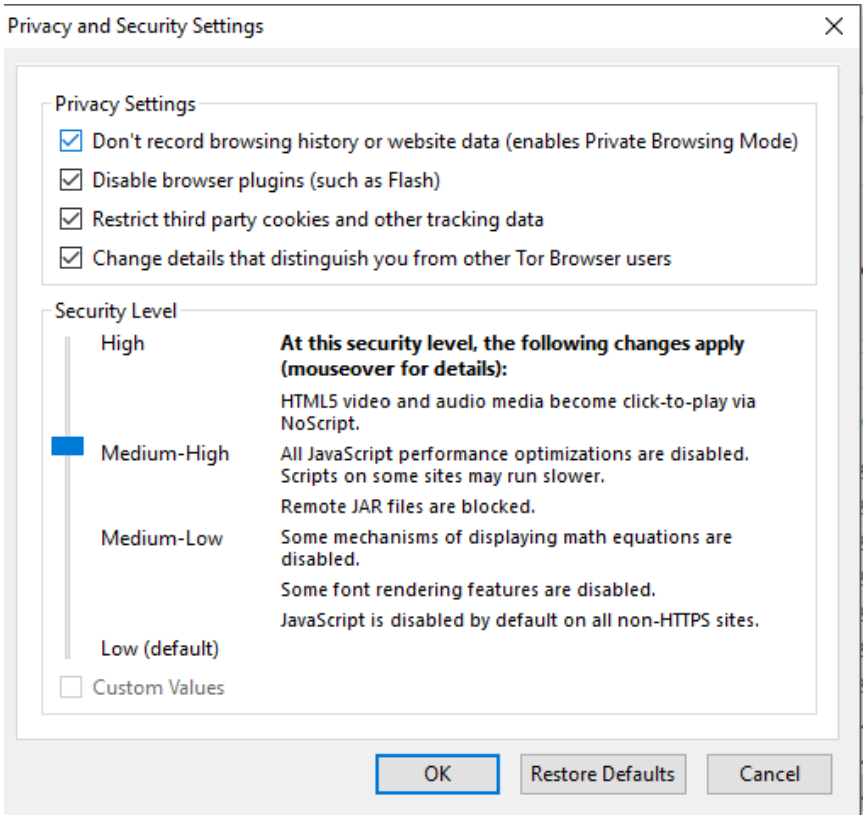


Slika 12. Najniže postavke privatnosti

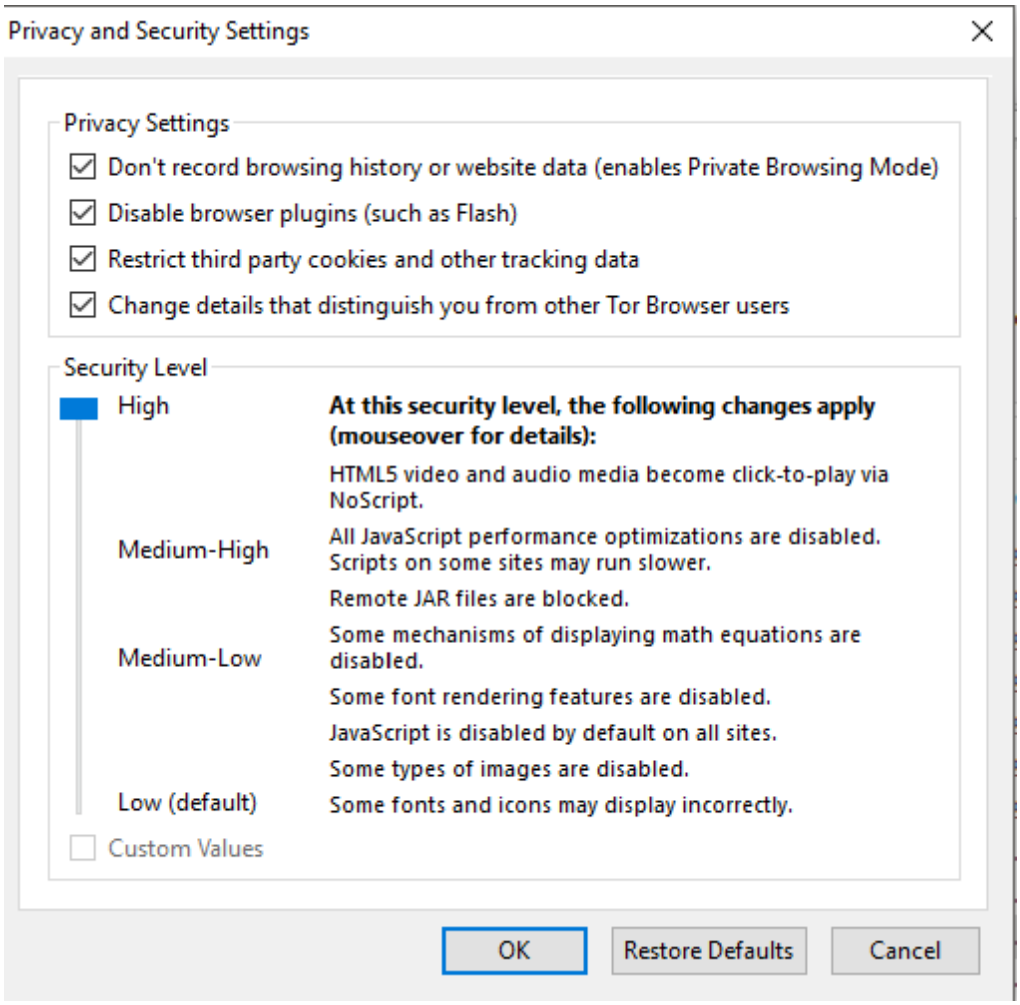
Od tih opcija po standardu je uključena najniža zaštita. Iako je pod tom opcijom sve uključeno, u daljnjim opcijama ima velikih razlika i napredaka naspram najniže zaštite. Omogućuje reprodukciju zvuka, videa, JavaScripta te pokretanje JAR datoteka.



Slika 13. Srednje niska sigurnost

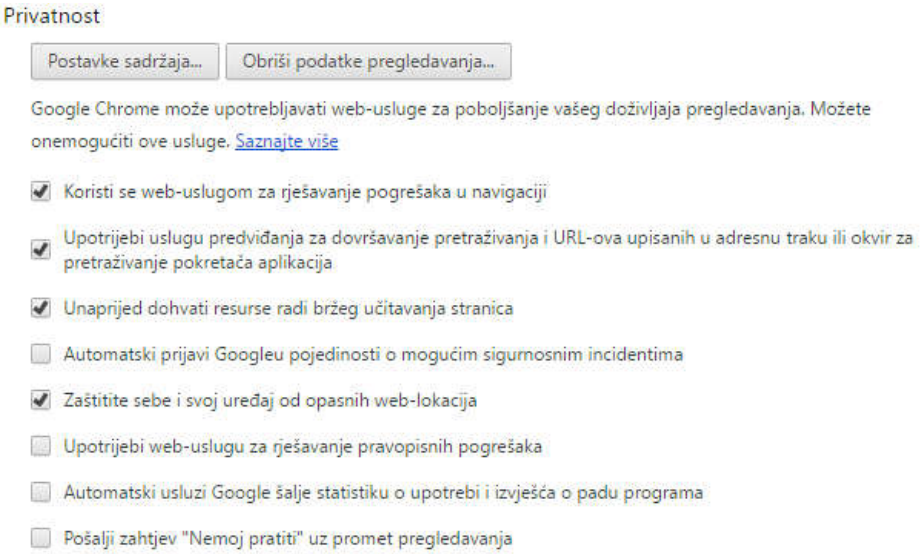


Slika 14. Srednje visoka sigurnost



Slika 15. Visoka sigurnost

Kao što je prikazano na slikama, zaštite se gotovo neprimjetno razlikuju jedna od druge, no kada se razina zaštite TOR pretraživača usporedi sa, npr. razinom zaštite Google Chromea, uočljive su velike razlike i razvijenost TOR-ovih postavki privatnosti.



Slika 16. Google Chromove postavke sigurnosti

Za razliku od Google Chroma, TOR pristupniku omogućuje potpunu kontrolu nad sadržajem koji on želi pregledati. TOR-ove postavke su postavljene na taj način da nema „rupe“ kroz koju bi mogli proći problemi. HTML5 video i zvuk nije moguće u potpunosti isključiti, niti ih postaviti da budu „click to play“. Java skripte su u potpunosti isključene, dok u Chromu uopće nema nikakvih postavki za JS.

3.3.Kako radi TOR

TOR u suštini koristi P2P (peer-to-peer) povezivanje. To je decentralizirani komunikacijski model u kojemu svaka stranka ima iste sposobnosti i svaka stranka može započeti komunikaciju s drugim strankama. Za razliku od modela server/klijent, u kojem klijent zahtijeva pristup serveru, koji može biti odobren ili odbijen, P2P model svim strankama u procesu daje mogućnost da se istovremeno ponašaju i kao server, i kao klijent.

Osim za komunikaciju, TOR se koristi i za kupovinu preko Interneta zbog svoje pojačane sigurnosti.

4. BitCoin

BitCoin je digitalnavaluta, koja se stvara i drži elektronički. Nitko nema kontrolu nad njime. Ne može se otiskivati poput eura, dolara ili ostalih valuta.Njega proizvode ljudi koji imaju posebni software i hardware za proizvodnju, kojimse rješavaju matematičke funkcije. Taj proces zove se BitCoin Mining.

Tvorac BitCoina je nedavno otkriveni Craig Wright.On je to potvrdio objavom informatičkog koda za BitCoin. Bio je poznatiji pod pseudonimom Satoshi Nakamoto . [20]

Njegov je cilj bio stvaranje valute koja je neovisna o bilo kakvoj centralizaciji, lako prenosivoj elektronički (manje više u sekundama) i svrlo niskom stopom poreza.

Bitno je da istovremeno u svijetu ne može biti više od 21 milijun BitCoina.Međutim, to ne mora biti cjelina, pošto se svaki BitCoin može raspodijeliti na manje dijelove koji su nazvani po tvorcu, Satoshi (1/100 000 000). [3]

4.1 Karakteristike

Bitcoin mreža nije kontrolirana ni od jednog centralnog autoriteta. Svaki stroj koji proizvodi BitCoin i procesira transakcije čini dio velike mreže koja radi zajedno sa svim povezanim računalima. Ako i dio mreže ode izvanmrežno, novac ostaje u toku. Dovoljno je samo unijeti e-mail adresu, bez ikakvih dodatnih pitanja(kao npr. kodbanaka) i bez ikakvog oporezivanja.

Korisnici mogu postaviti više e-mail računa s ciljem povećavanja anonimnosti. Problem je u tome što je anonimno i u isto vrijeme transparentno. Tako se preko „blockchaina“ može vidjeti koliko je BitCoina spremljeno na nekoj e-mail adresi, ukoliko je adresa korištena javno. Naravno, ime vlasnika nije vidljivo.

Za međunarodne prijenose, banke naplaćuju barem 10€. BitCoin, naprotiv, ne naplaćuje ništa. Transakcija novca BitCoinom je gotova, najkasnije onog trena kad elektronički signal dospije na mrežu, bez ikakvih posebnih procedura. BitCoin nije povratan ukoliko osoba ili tvrtka kojoj se isplatilo ne želi sama vratiti novac. [3]

4.2 Utvrđivanje cijene Bitcoina

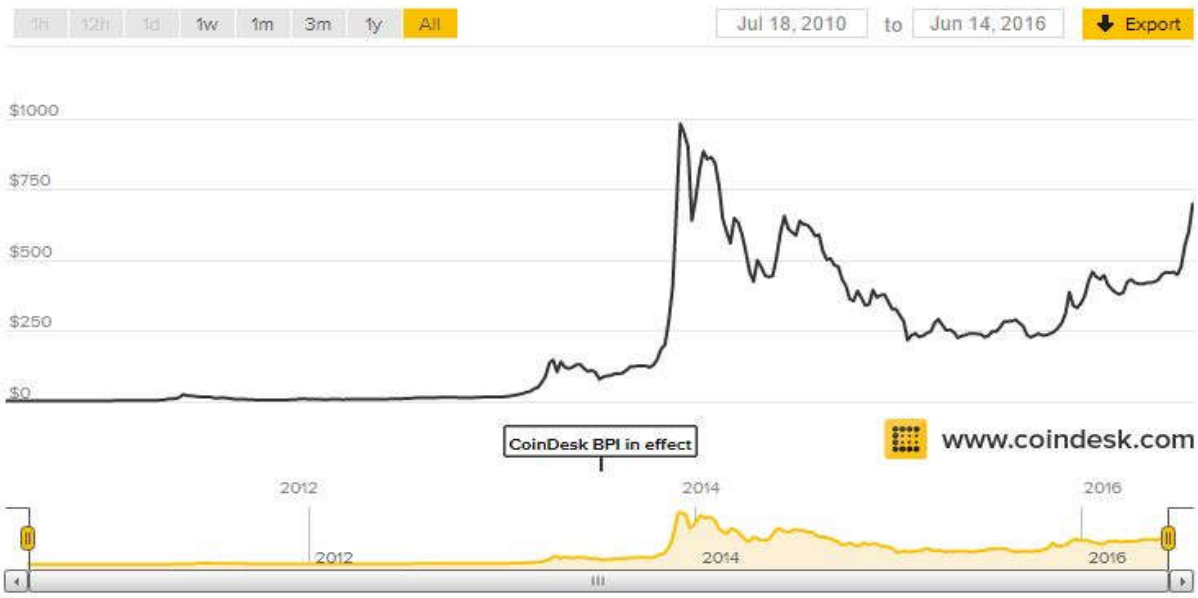
BitCoin mreža ne može biti ugašena, baš kao ni BitTorrent ili bilo koja slična web usluga, jednostavno zato što nije ovisna ni o kakvom vanjskom autoritetu, niti ičijem mišljenju, niti ikakvoj akciji.

Kao i kod svake valute, visina cijene BitCoina utvrđuje se ponudom i potražnjom. Dakle, cijena BitCoina je viša ukoliko je potražnja za njega velika iniža ukoliko je velik broj BitCoina u opticaju. Isto tako, kriza u drugim valutama ne utječe na njegovu cijenu. Ne postoje banke BitCoina, već svaki korisnik sam utječe na svoj račun,čime je sam odgovoran za sigurnost i način upravljanja.

BitCoin je zapravo kod koji se sastoji od slova i brojeva i sprema se na BitCoin adresu. Adresa BitCoina ima oblik tipa „19Ms9LtcqAJ1u436e9kjnyzkkLy18EQuBY“ .

BitCoin se kao kod može kopirati više puta, međutim, može se samo jednom potrošiti. Takav dizajn se može provjeriti na način da se već postojeći BitCoin novčanik kopira i prebaci na drugo računalo. Tim prebacivanjem drugi korisnik bi isto mogao upravljati tim računom, no samo prva transakcija može biti uspješna. Iako postoji već godinama, BitCoin je još uvijek u razvoju pod licencom MIT-a. [4]

Današnja cijena pojedinačnog BitCoina je 684.74 $, dok je njegova najveća cijena od puštanja u opticaj bila približno 979$.

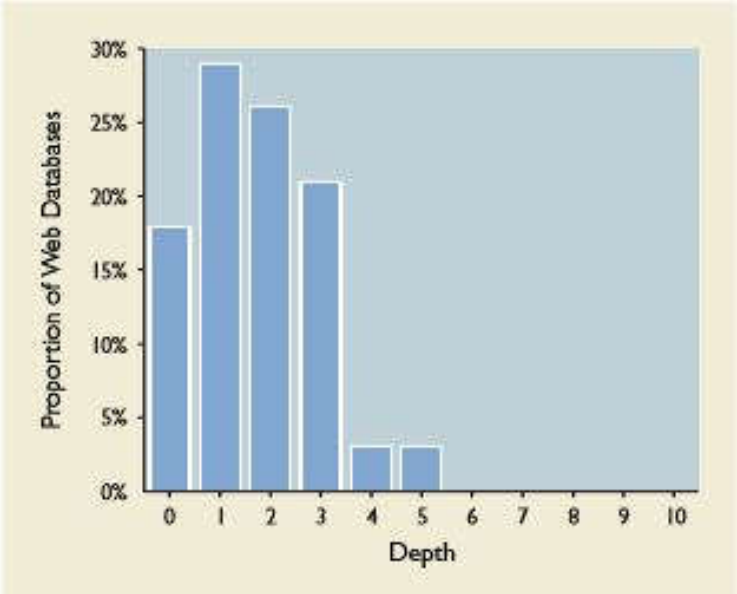


Slika 17. Rast vrijednosti BitCoina od postanka do današnjeg dana.[5]

5.Istraživanja o Deep Webu

Tokom posljednjih 15 godina napravljeno je više studija o samoj veličini Deep Weba. Nitko nije mogao procijeniti točnu veličinu te se ispostavilo sljedeće.

Najopširnije istraživanje iz 2007. godine postavilo je standard za dubinu Deep Weba. [6]



Slika 18. Razine dubine Deep Weba [6]

Postavili su „query“ , čime su dobili da ni jedan od svih dobivenih 129 upita nije „dublji“ od dubine 5.
Od toga je 72% (93 od 129) sučelja pronađeno unutar dubine 3,njih 94%(32 od 34) je imalo baze podataka najmanje unutar dubine 3, dok je 91.6 % (22 od 24) imalo baze podataka unutar dubine 3.[6]

Istraživanje je provedeno na način da se testiralo 1 000 000 IP uzoraka za određivanje razmjera Deep Weba.

Tablica 1 Rezultati istraživanja 2 [6]

	Rezultati uzoraka	*Ukupna procjena*	*Interval podudarnosti od 99%*
Stranice Deep Web	126	307,000	236,000-377,000
Web baze podataka	190	450,000	366,000-535,000
-nestruktrurirane	43	102,000	62,000-142,000
Strukturirane	147	348,000	275,000-423,000
Upitna sučelja	406	1,258,000	1,097,000-1,419,000

Prema istraživanju koje su izvršili, dobiveni rezultati pokazali su da seDeep Web povećao od 3-7 puta u razdoblju između 2000. i 2004. godine. Uza sve to Deep Web ima razmjer od 307,000 stranica, 450,000 baza podataka i 1,258,000 sučelja. Različitost sadržaja mijenja se kroz svaku stranicu, iako su najpopularniji sadržaj bile e-reklame. Izvori podataka na Deep webu većinom su strukturirani, 3.4 puta češće nego nestrukturirani izvori, za razliku od "Visible Weba". Čak 94% Deep Web baza podataka je spremljeno na dubinu 3. Ostalih 6 % nije bilo moguće pronaći. [6]

U istraživanju je bio korišten jedan od Web Crawler programa. To je program koji automatski skida web stranice. On funkcionira tako da se postavi neka početna adresa, koja nakon preuzimanja povezuje druge adrese na koje je moguće doći preko nje. Većina servera pokrenuta je preko Apachea, tako da Apache server mora biti kompatibilan sa Crawlerom da ispravno radi. To je objasnio i Onn Brandman u svojem istraživanju Crawler-Friendly Web Servers. [7]

6. Zaključak

Internet je u globalu moguće grubo kategorizirati na tri dijela. Prvi je najzastupljeniji jer je dostupan najjednostavnijom uporabom Internet pretraživača (npr. Google, Bing, Yahoo…) kojima pristupamo pomoću programa koji su danas standard svih računala i mobilnih uređaja (npr. Chrome, Opera, Internet Explorer…). Taj dio poznat je kao površinski web i koriste ga ljudi za svakodnevno pretraživanje informacija i komunikaciju.

Drugi dio je bolje osiguran i sakriven, a sastoji se od raznih bankovnih i medicinskih dokumenata, znanstvenih istraživanja i mnogih drugih sadržaja koji su legalni, ali pristup nije omogućen široj javnosti. U tom se dijelu nalaze sve baze podataka koje korisnici ne žele izgubiti, ali ne mogu ih ni objaviti široj javnosti iz raznih razloga, prvenstveno sigurnosti.

Treći, najdublji dio Interneta, sadrži većinom ilegalne podatke. Najpoznatiji je pod nazivom Dark Web, a njegovi korisnici se bave raznim kriminalnim radnjama.

U virtualnom svijetu Deep Weba kao valuta za plaćanje koristi se BitCoin. Ta elektronička valuta u potpunosti je nepovezana s drugim valutama svijeta, ali izračunava se na istom principu prilagođavajući se potražnji. Svaki BitCoin ima svoju adresu i nije ga moguće povezati s njegovim kupcem.

Pristup Deep Webu je kompliciraniji od pristupa površinskom webu, ali opet je zastupljen kod velikog broja korisnika i čini preko 90% sadržaja ukupnog Interneta. Sadržaj je dostupan tek pretraživanjem pomoću posebnog pretraživača TOR-a koji garantira sigurnost i anonimnost korisnika. Najsigurnije ga je koristiti sa OS Linux Tailsom.

Ono što je e-Bay „običnom“ korisniku, to je Silk Roadbio korisnicimaDark Weba. Na njemu su se prodavala sva dobra koja je netko mogao pronaći, razna opojna sredstva, vatreno oružje, pa čak i usluge poput unajmljivanja ubojica. Nakon njegovog gašenja nastale su mnoge nove inačice tog „crnog tržišta“.

Dobru stranu Deep weba čine sigurnosne službe i druge agencije (FBI, NSA, privatni špijuni, istraživači te novinari) koji pridonose u razotkrivanju svih ilegalnih aktivnosti. Usprkostrudu sigurnosnih služba u borbi protiv kriminala putem Deep Weba, njegov broj korisnika i količina protoka informacija u stalnom su rastu.

U želji za materijalnom koristi, pogotovo u vrijeme recesije, krize i sve većeg siromaštva, ljudi se sve više upuštaju u ilegalne aktivnosti, a Deep Web je samo alat koji im to omogućuje i to na relativno jednostavan i siguran (anoniman) način.

Reference

[1] http://www.news.com.au/technology/online/what-is-the-deep-web-and-anonymous-browser-tor/story-fnjwnfzw-1226844901718

[2] https://en.wikipedia.org/wiki/Tor_(anonymity_network)

[3] http://www.coindesk.com/information/what-is-bitcoin/

[4] https://www.cryptocoinsnews.com/determines-value-bitcoin/

[5] http://www.coindesk.com/price/

[6] Accessing the Deep Web, Bin He, Mitesh Patel, Zhen Zhang and Kevin Chen-Chuan Chang, Communications Of The ACM, May 2007.

[7] Crawler-Friendly Web Servers, Onn Brandman, Junghoo Cho, Hector Garcia-Molina, Narayanan Shivakumar, ACM SIGMETRICS, Volume 28 Issue 2, Sept 2000.

[8] https://en.wikipedia.org/wiki/Silk_Road_(marketplace)

[9] Dokumentarni film"Deep Web", Alex Winter

[10] https://www.gwern.net/Silk%20Road

[11] http://www.forbes.com/sites/kashmirhill/2013/10/17/does-this-17-million-bitcoin-wallet-belong-to-alleged-silk-road-mastermind-ross-ulbricht/#230bba815385

[12] Inside the Dark Web, PC MAGAZINE DIGITAL EDITION, Veljača 2015

[13] https://blockchain.info/wallet/paypal-vs-bitcoin

[14] http://www.businessinsider.com/bitcoin-versus-paypal-comparison-2013-12

[15] https://gnunet.org/

[16]https://en.wikipedia.org/wiki/History_of_the_Internet

[17] A Review Paper on Deep Web Data Extraction using WordNet,Nagesh Kumar Jha, Aakash Jethva, Nidhi Parmar , Professor Abhay Patil ,International Research Journal of Engineering and Technology, Volume: 03 Issue: 03, Mar-2016 (https://www.irjet.net/archives/V3/i3/IRJET-V3I3217.pdf)

[18] http://www.independent.co.uk/news/world/europe/eric-eoin-marques-28-year-old-architect-s-son-from-dublin-accused-of-being-world-s-biggest-dealer-in-8782756.html

[19] http://www.gwern.net/Black-market%20archives

[20] http://www.bbc.com/news/technology-36168863

Sveučilište
Sjever

IZJAVA O AUTORSTVU
I
SUGLASNOST ZA JAVNU OBJAVU

Završni/diplomski rad isključivo je autorsko djelo studenta koji je isti izradio te student odgovara za istinitost, izvornost i ispravnost teksta rada. U radu se ne smiju koristiti dijelovi tuđih radova (knjiga, članaka, doktorskih disertacija, magistarskih radova, izvora s interneta, i drugih izvora) bez navođenja izvora i autora navedenih radova. Svi dijelovi tuđih radova moraju biti pravilno navedeni i citirani. Dijelovi tuđih radova koji nisu pravilno citirani, smatraju se plagijatom, odnosno nezakonitim prisvajanjem tuđeg znanstvenog ili stručnoga rada. Sukladno navedenom studenti su dužni potpisati izjavu o autorstvu rada.

Ja, NEVEN DAGO *(ime i prezime)* pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor/ica završnog/diplomskog *(obrisati nepotrebno)* rada pod naslovom DEEP WEB *(upisati naslov)* te da u navedenom radu nisu na nedozvoljeni način (bez pravilnog citiranja) korišteni dijelovi tuđih radova.

Student/ica:
(upisati ime i prezime)
Neven Dago
(vlastoručni potpis)

Sukladno Zakonu o znanstvenoj djelatnost i visokom obrazovanju završne/diplomske radove sveučilišta su dužna trajno objaviti na javnoj internetskoj bazi sveučilišne knjižnice u sastavu sveučilišta te kopirati u javnu internetsku bazu završnih/diplomskih radova Nacionalne i sveučilišne knjižnice. Završni radovi istovrsnih umjetničkih studija koji se realiziraju kroz umjetnička ostvarenja objavljuju se na odgovarajući način.

Ja, NEVEN DAGO *(ime i prezime)* neopozivo izjavljujem da sam suglasan/na s javnom objavom završnog/diplomskog *(obrisati nepotrebno)* rada pod naslovom DEEP WEB *(upisati naslov)* čiji sam autor/ica.

Student/ica:
(upisati ime i prezime)
Neven Dago
(vlastoručni potpis)