Analiza BitTorrent protokola pomoću analizatora mrežnog prometa

Primorac, Danijel

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Stručni studij

ANALIZA BITTORRENT PROTOKOLA POMOĆU ANALIZATORA MREŽNOG PROMETA

Završni rad

Danijel Primorac

Osijek, 2016. godina.

Sadržaj

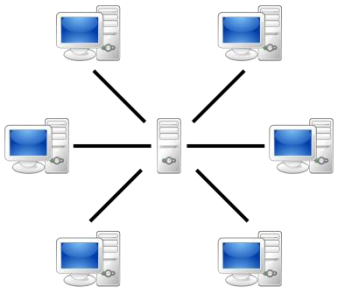
1. UVOD

Peer-to-peer (u daljnjem tekstu P2P) popularan je način razmjene podataka i informacija među korisnicima, naime to je mreža u kojoj nema klijent-server modela i servera. Svi su čvorovi u P2P modelu hijerarhijski jednaki, te ne postoji glavno računalo niti server koji nadgleda koji podaci se dijele u mreži. Za takvu razmjenu podataka u P2P mrežama koriste se P2P protokoli a u ovom slučaju pobliže će se objasniti BitTorrent protokol. BitTorrent protokol često se naziva BitTorrent datotekom što je pogrešno jer je BitTorrent protokol kojim se vrši razmjena podataka dok je sami naziv datoteke torrent (te ima i naziv ekstenzije torrent). BitTorrent je P2P protokol za distribuiranu razmjenu datoteka. Omogućava distribuciju velike količine podataka bez prisustva originalnog izvora. Kada su podatci distribuirani pomoću BitTorrent protokola, svaki klijent pruža dio datoteke novom klijentu, smanjujući tako opterećenje izvora. Osnovna ideja je da se datoteka podijeli na manje dijelove (pieces). Kako bi se uštedjelo na opterećenju, svaka osoba (peer) koja preuzima (download) dijelove nekog sadržaja, automatski omogućuje njihovo preuzimanje ostalim peerovima u gomili (swarm). Prema nekim procjenama BitTorrent čini čak 35% od ukupnog prometa na Internetu danas iako je točan postotak dosta teško utvrditi sa točnošću. BitTorrent klijent je bilo koji program koji implementira BitTorrent protokol. Svaki BT klijent ima mogućnost pripremanja, traženja tj. zahtijevanja i slanja datoteka koristeći protokol. Peer je računalo na kojem je pokrenuta klijentska aplikacija. Kako bi se što bliže prikazalo i pojasnilo kako se BitTorrent protokol primjenjuje u svakodnevnom svijetu koristit će se program Wire-Shark i uTorrent te s pomoću njih analizirati nekakav torrent na webu.

2. PEER TO PEER MREŽA

2.1 Peer to peer mreže

Peer to peer je računalna mreža koja podrazumijeva umrežavanje i komunikaciju računala bez prisustva poslužitelja u kojoj je svako računalo kao nekakva ravnopravna stanica u mreži koja se povezuje sa drugim računalima i s njima izravno komunicira te dijeli datoteku, a da pri tome ne traži nikakvo odobrenje (Sl. 2.2). Ovakav model mreže razlikuje se od klijent-server modela prema slici 2.1, gdje se cijela komunikacija odvija preko centralnog poslužitelja [1].



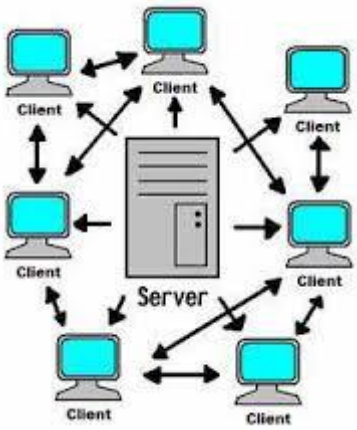
Sl. 2.1 Klijent - server model

Sl. 2.2 P2p model

2.2 Generacijski razvoj p2p mreža

P2p mreže se prema strukturi dijele na centralizirane i decentralizirane dok se decentralizirane mreže mogu još dijeliti na strukturirane i nestrukturirane. Dalje slijedi pregled svake od mreža kao i njezina osnovna svojstva.

Prva generacija su centralizirani p2p sustavi kao što i sama riječ govori radi se o centralnom poslužitelju koji usmjerava promet između registriranih korisnika vidljivo prema slici 2.3. Središnji poslužitelji održavaju direktorije sa dijeljenim datotekama koje su pohranjene na računalu korisnika. Datoteke kao takve nikada nisu pohranjene na centralnom poslužitelju. Svaki puta kada neki korisnik zatraži nekakvu određenu datoteku, centralni poslužitelj pretražuje istu na popisu dostupnih mu datoteka od trenutno spojenih korisnika. Nadalje poslužitelj prikazuje korisniku listu trenutno dostupnih datoteka te korisnik kao podnositelj zahtjeva, odabire od koga će preuzeti datoteku te se samim time uspostavlja HTTP konekcija između oba korisnika i počinje prijenos. Primjer mreže prve generacije je Napster koji je bio korišten za razmjenu glazbe u MP3 formatu. Napster je bio on line usluga koju je stvorio Shawn Fanning, radila je u periodu od 1999.-2001. te je u konačnici zaustavljena od strane američkih sudova zbog kršenja autorskih prava ili druge ilegalne radnje. Rezultat gašenja takve usluge otvara put decentraliziranom p2p sustavu kojega je puno teže držati pod kontrolom.



Sl. 2.3 *Centralizirani sustav*

Glavne prednosti centraliziranog sustava je postojanje tablica, u kojoj se nalazi popis datoteka te se one mogu brzo i jednostavno pronaći, te se ista konstantno osvježava pa je nakon pretrage moguće odmah preuzeti datoteku. Jedna od prednosti svakako je ta što se korisnici moraju registrirati tako da se pretraživanje obavlja samo nad ulogiranim korisnicima. Druga strana medalje ovakvog sustava je sasvim logična, a to je da centralizirani sustav ima samo jednu ulaznu točku tj. poslužitelja i ako se on odsječe, past će cijeli centralizirani sustav [2].

Druga generacija p2p mreža donosi potpunu decentralizaciju. Svi su klijenti postali međusobno ravnopravni te su pretraživali i dijelili datoteke, bez ikakve ulazne točke tj. servera, tako da

svako računalo ili peer istovremeno šalje i prima podatke za razliku od veze tipa server-klijent. Primjer ovakve mreže je Gnutella, jedna od najpopularnijih mreža za razmjena podataka na internetu [2].

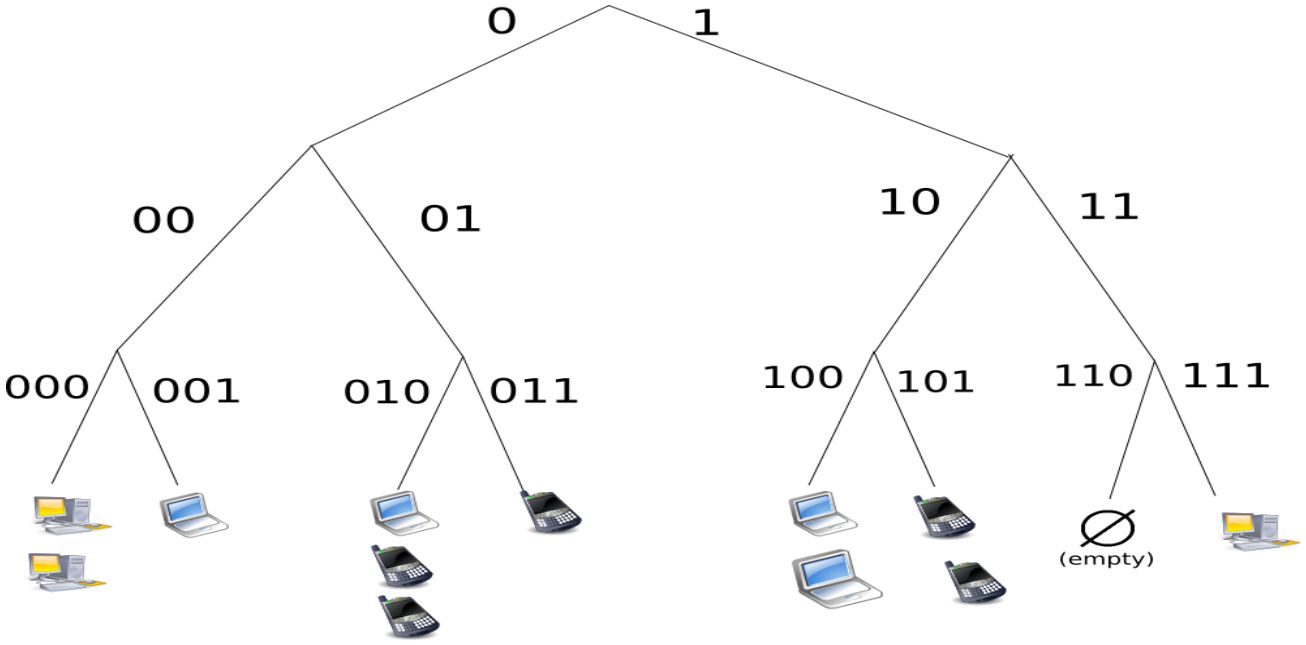
Treća generacija p2p mreža uvodi kriptiranje podataka i anonimnost. Primjer treće generacije je BitTorrent protokol kojeg razvija Bram Cohen, napravljen je da olakša distribuciju velikih dokumenata te se sav promet odvija između izvora dokumenta (seed) i onoga koji taj isti dokument preuzima (leecher) [2].

2.3 Arhitektura p2p mreža

P2P mreže prema strukturi se dijele na centralizirane i decentralizirane. U nastavku je pregled osnovnih svojstava svake od mreža.

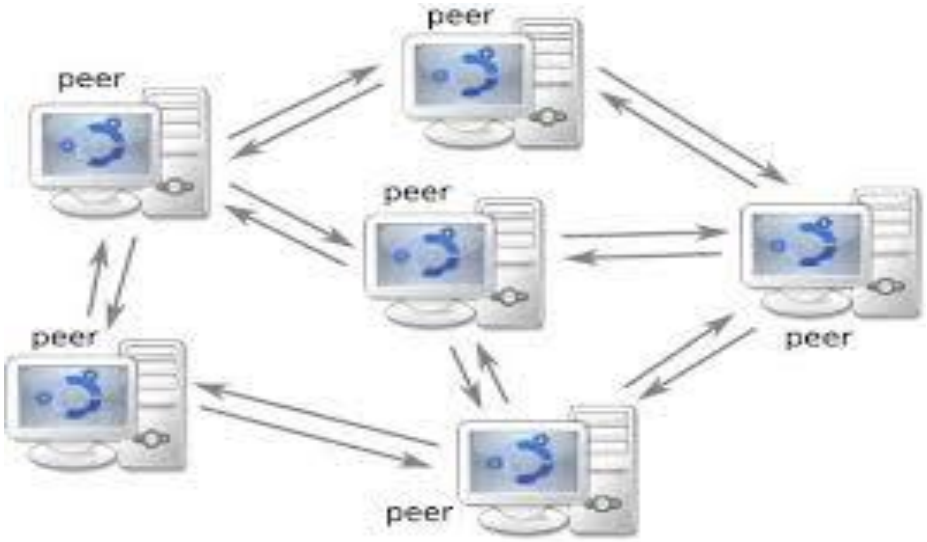
Centralizirane p2p mreže kao i njihova osnovna svojstva navedena su u prethodnom potpoglavlju tako da se neće ponavljati, već se može spomenuti da su primjeri ovakve mreže bili Freenet i prva verzija Gnutelle.

Decentralizirane p2p mreže se dalje dijele na **strukturirane** i **nestrukturirane**. Kada se govori o **strukturiranim** p2p sustavima vidljivo prema slici 2.4, govori se o sustavima koji imaju definiranu mrežnu topologiju, te imaju točno određen mehanizam za traženje određenih podataka. Drugim riječima, podaci su spremljeni na točno određenim lokacijama. Kako imamo definiranu mrežnu topologiju dolaskom novih podataka i klijenata mehanizam se prilagođava. Jedan od načina na koji se to postiže je pomoću hash funkcije na imenima podataka i čvorova, dakle podatke se postavi na čvorove koji imaju približno sličnu hash vrijednost kao i dani podaci. Kada se traži određeni podatak u ovakvoj mreži to je brzo i efikasno, no ovakve strukture imaju velike probleme kod prilagođavanja novom klijentu i podatku. Za primjer navedene strukture je Chord protokol, jedan od prvih koji koristi hash funkciju i ovakvu strukturu [1].



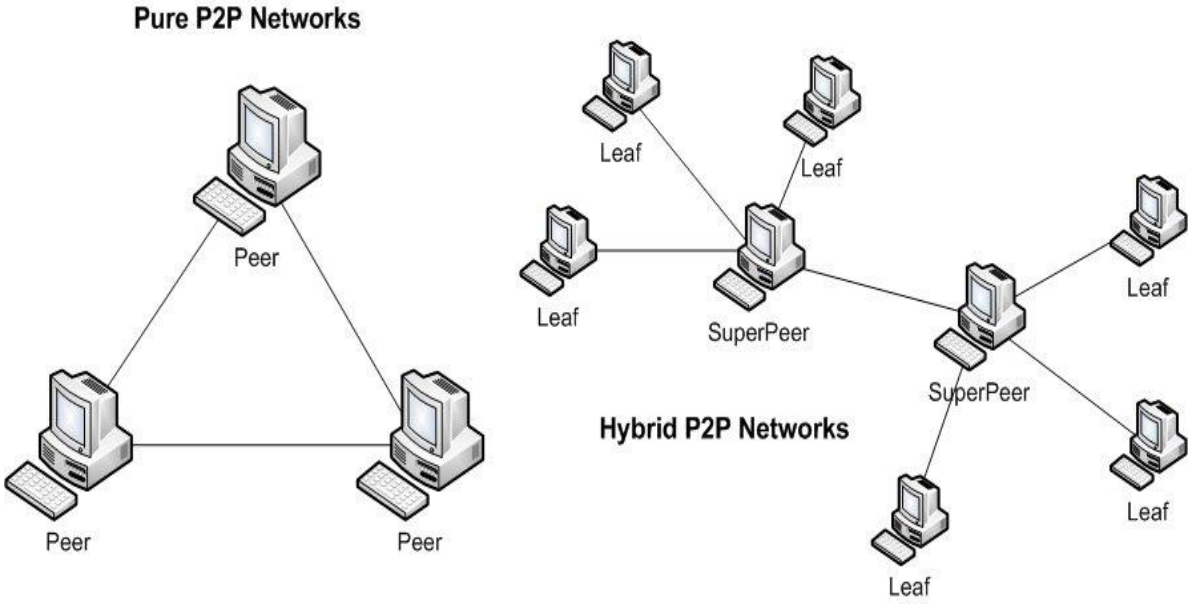
Sl. 2.4 Strukturirani p2p

Nestrukturirane p2p mreže, za razliku od strukturiranih sustava, mrežna topologija nema definiranu strukturu (Sl. 2.5), tako da je mreža peer-ova slučajan graf, dakle podaci koji se nalaze na pojedinom čvoru su proizvoljni. Kada se pretražuj određeni podatak, najčešće se mora obići veliki broj čvorova jer ne znamo gdje se točno nalazi traženi podatak. Takvi sustavi, kao način pretrage, često koriste emitiranje kojim se šalje upit na susjedni čvor i dalje redom dok se ne prođu svi čvorovi ili dok se ne pronađe određeni podatak. Upravo je to velika zamjerka ovakvih sustava, jer kada dođe do velikog broja upita dolazi i do preopterećenja mreže. Opet, prednost je ta ako se bilo koji čvor ugasi ili pokvari sustav neće pasti već će se samo prilagoditi i nastaviti dalje sa radom u odnosu na centralizirani sustav koji pada jer nema ulazne točke. Primjer ovakvog sustava je već spomenuta Gnutella koja u svom primjeru koristi ograničen broj pretraženih čvorova za nekakav podatak, što znači da se svaki zahtjev ne razašilje beskonačno dugo svim susjedima pojedinog čvora, naravno sa izuzećem onoga koji je zahtjev poslao, već se takvo gušenje mreže provodi u točno određenom broju koraka. Kod Gnutelle je taj broj koraka postavljen na 7 te uz poznavanje činjenice da svaki čvor do kojeg dođe upit umanji vrijednost za 1. Uz ovakav način pretrage čvorova postoji velika vjerojatnost da će se nekakav zahtjev pozitivno obraditi bez da pretjerano zakrči mrežu [1].



Sl. 2.5 Nestrukturirani p2p

Hibridne p2p mreže su mješavina centraliziranih i decentraliziranih sustava. Hibridni sustav dopušta postojanje tzv. "superčvorova" koji su gotovo isti kao i "obični" čvorovi, no imaju značajnu ulogu kod pretrage za neki određeni podatak (Sl. 2.6). Ovdje hibridni sustavi posjeduju jedan dio centraliziranog sustava a to je gdje poslužitelj ima bazu podataka tako i "superčvorovi" uzmu dio "običnih" čvorova iz mreže i naprave listu datoteka sakupljenih iz istih čvorova. Kada čvor traži određeni podatak šalje upit svome "superčvoru" koji gleda u svoju bazu podataka tj. listu i ukoliko ne posjeduje isti vrši emitiranje među ostalim čvorovima. Dakle klijent-server arhitektura se koristi za pretraživanje datoteka, a čisti p2p na njihov prijenos. Primjeri ovakve mreže su Gnuella2 (moderna implementacija Gnutelle) i Kazaa [1].



Sl. 2.6 Obični i hibridni p2p

3. BITTORRENT PROTOKOL

3.1.Kako radi torrent

Torrent je centralizirana p2p mreža koja je u mogućnosti točno prikazati koju datoteku netko dijeli, unatoč ostalim datotekama istog imena ili veličine. Skida se točno određena datoteka bez obzira koliko drugih datoteka postoji sa istim karakteristikama. Takav podatak se pohranjuje unutar male tekstualne datoteke koja ima ekstenziju *.**torrent** te također sadrži podatke o serveru koji upravlja skidanjem datoteke.

Datoteka koja se skida preko torrent mreže podijeljena je u blokove koji se kreću od 32kB do 4096kB, dok je svaki od blokova podijeljen na pakete tako da jedan blok sadrži 8 paketa. U teoriji optimalna komunikacija tj. razmjena podataka se može istovremeno obavljati sa 4 klijenta od kojih prva 3 budu odabrani po brzini kojom mogu slati podatke, omjeru dijeljenja tj. **share ratio** te prisutnosti podataka koje tražimo, dok se 4. klijent bira nakon svaka 3 ciklusa osvježavanja podataka. Prva 3 klijenta se konstantno provjeravaju i osvježavaju svakih 5 minuta.

Naravno kao i uvijek brzina je najvažnija i najrizičnija stavka Bittorrent protokola jer nema servera sa kojeg bi skidali podatke velikom brzinom, već te iste servere zamjenjuju korisnici Bittorrent protokola (korisnici koji u tom trenutku skidaju sadržaj). Poželjno bi bilo pri skidanju datoteke putem Bittorrent mreže da se postigne što veći share ratio tj. da bude veći ili jednak 1 (koliko podataka skinemo toliko ih i pošaljemo) jer osiguravamo veću brzinu rada mreže kao i pouzdanost. Idealno bi bilo nakon što se preuzme, datoteku ostaviti da se seed-a još neko vrijeme.

Bitan zaključak je to da pri skidanju nekog sadržaja brzina ovisiti o omjeru seeder-a i leecher-a, zatim slijedi brzina vaše Internet veze te na kraju postavke programa sa kojim se preuzima sadržaj. Cilj je postići što više seeder-a, a što manje leecher-a.

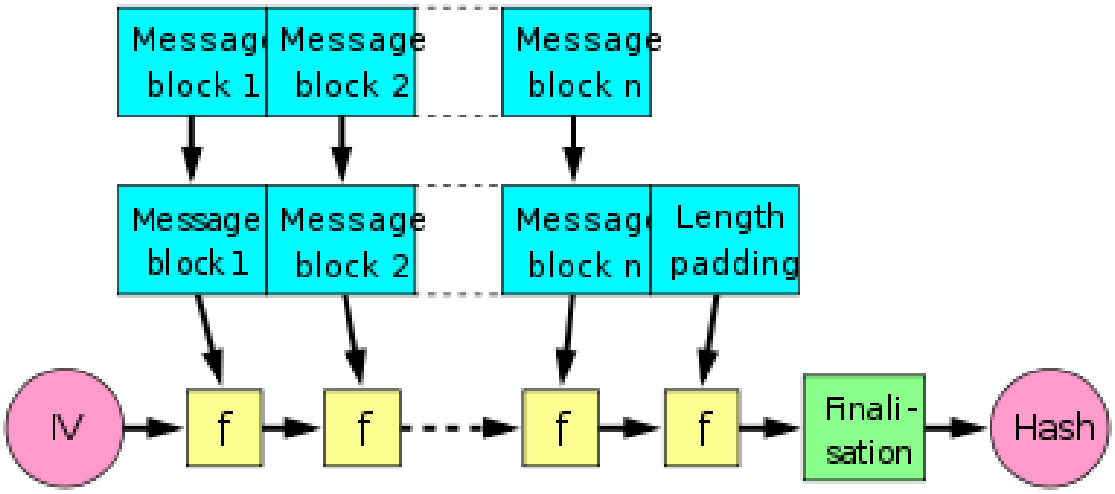
Torrent-e se dijeli na dvije vrste: javni (public) koji je dostupan svima i privatni (private) dostupan samo onima koji se registriraju na određenoj stranici. Kod javnih, brzine skidanja su puno manje jer korisnici koji skidaju ne mare za omjer download-a / upload-a, ali prednost je svakako puno datoteka različitog sadržaja. Kod privatnih torrent-a brzina skidanja je na maksimumu, jer torrent-i imaju konstantne korisnike koji upload-aju određene datoteke, dok je mana nedostatak datoteka.

Neki od poznatijih torrent-a su svakako: "The Pirate Bay", "Kickass Torrents", "Torrentleech.org", "Isohunt" (Sl. 3.1).

Slika 3.1 Razni torrent-i

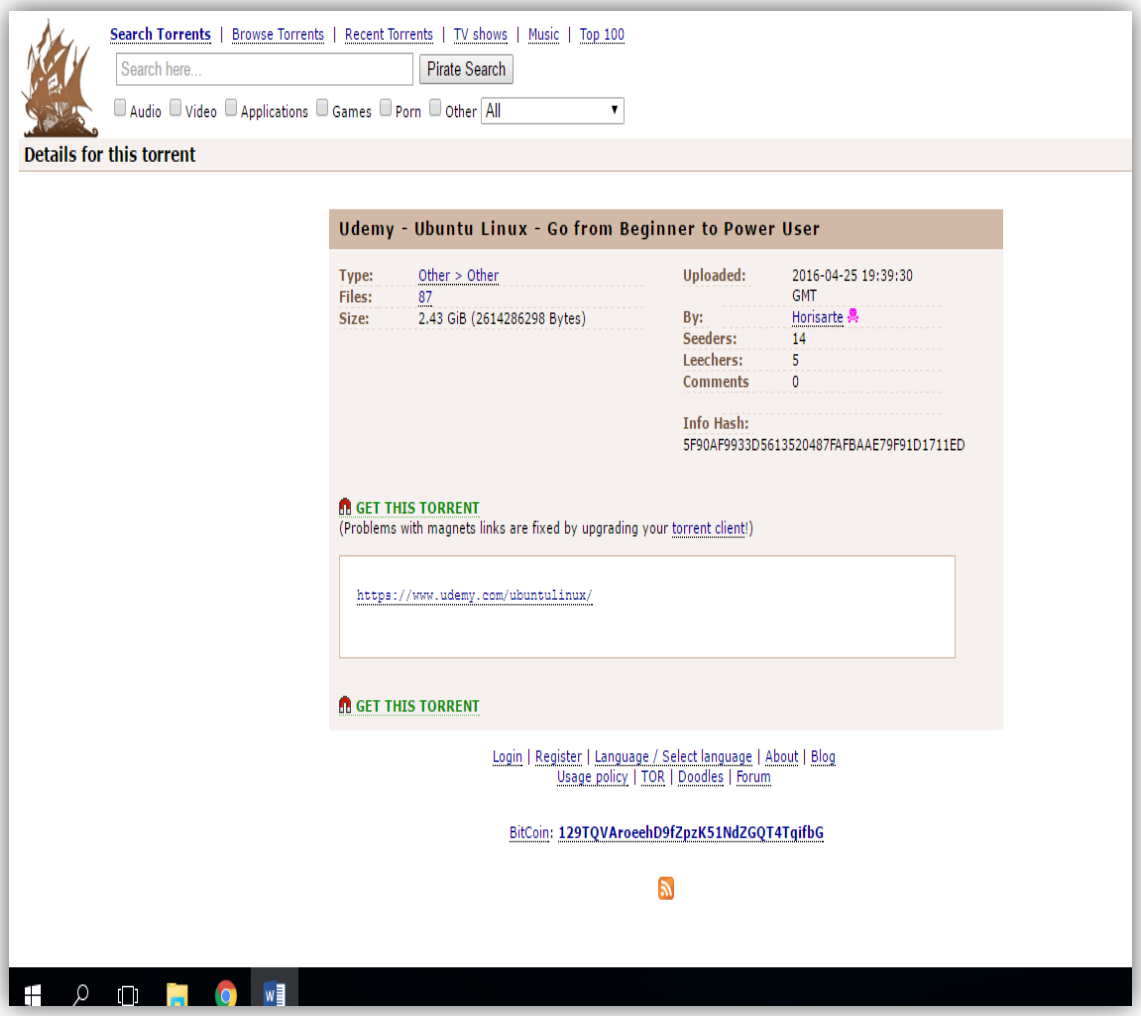
3.2 Stvaranje i objavljivanje torrent-a

Datoteke koje se žele dijeliti moraju se prvo indeksirati, dakle datoteka se dijeli na jednake dijelove od 16kB pa sve do 4MB, te se odrađuje SHA-1 algoritam svih dijelova (Sl. 3.2). Veći dijelovi se uzimaju kod velike količine podataka, dok je kod manjih količina podataka manji te se dobiva torrent koji je više podijeljen te ga je kao takvog lakše dijeliti između ostalih korisnika.



Sl. 3.2 Prikaz strukture podataka unutar torrent-a

Naravno kako bi se klijent osigurao da je primio kompletan dio određene datoteke radi se zaštitni dio svakog dijela datoteke te se zaštitni dijelovi uspoređuju i ako su isti ispravni prihvaća se, ipak ako ne odgovaraju taj se dio datoteke odbacuje i ponovno se pretražuje isti. Na kraju se dobivena datoteka snimi na poslužitelj torrent datoteka. Nakon toga korisnik koji dijeli određenu datoteku javlja se na tracker poslužitelj i tada svi ostali korisnici koji su pronašli torrent na indeks-poslužitelju počnu dijeliti datoteku, prvo od izvora, a poslije i međusobno. Formati torrent datoteke ovise o verziji Bittorrent protokola ali najčešće je sufiks .torrent. Torrent se sastoji od svojeg "oglašivaćkog" dijela u kojem se nalazi URL posrednika te "info" dio gdje se nalaze imena datoteka, njezina duljina, veličina dijela, te zaštitni dio za svaki djelić (Sl.3.3). Torrent datoteke se nalaze na raznim web stranicama i registrirane su na posredniku. Posrednik je taj koji sadrži listu klijenata koji trenutno sudjeluju u prijenosu datoteke [3].



Sl. 3.3 Detalji o torrent-u

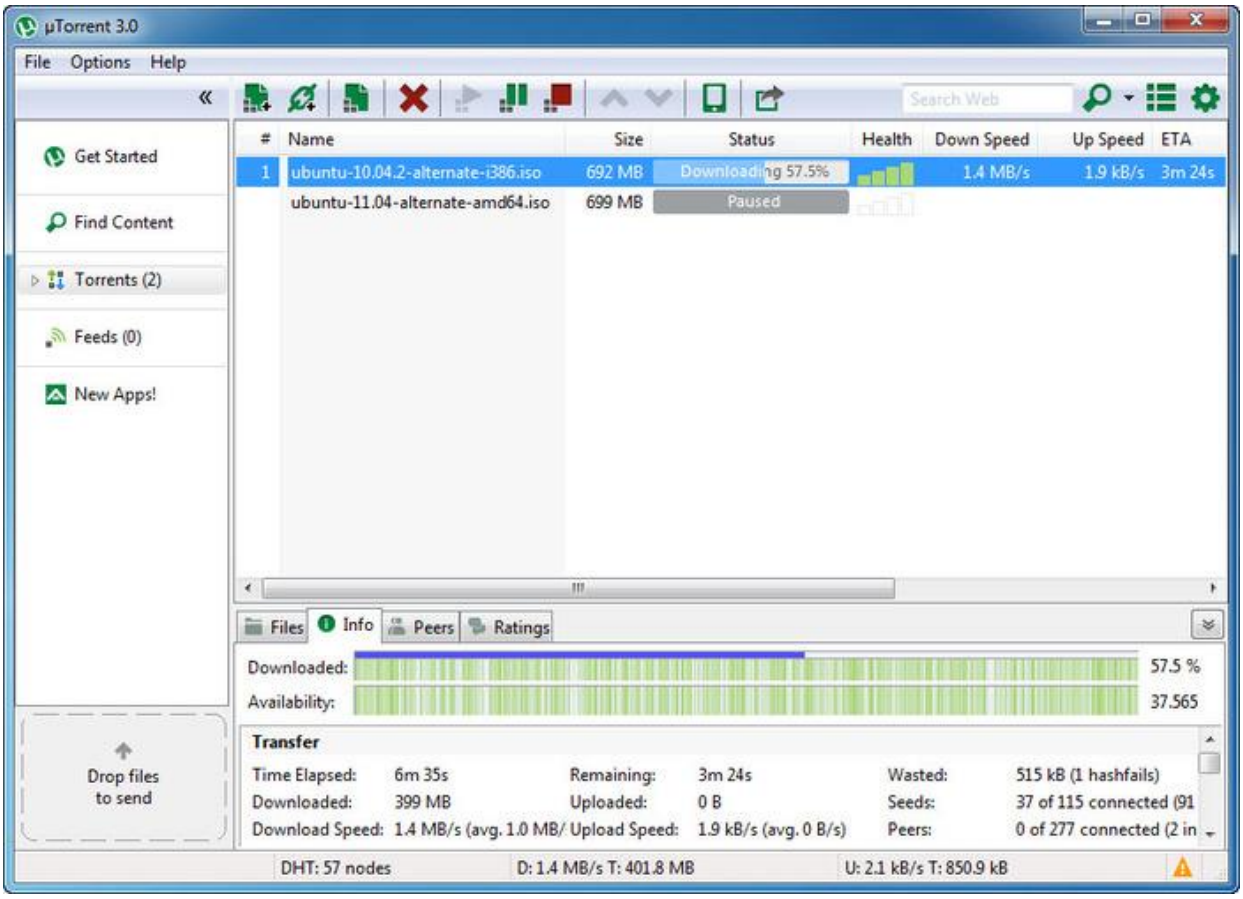
3.3 Dohvaćanje torrenta i dijeljenje datoteka

Pretragom interneta korisnici traže određenu torrent datoteku vidljivo prema slici 3.4, dohvate te pokrenu u lokalnom Bittorrent klijentu prema slici 3.5. Kako bi klijent počeo skidati određene datoteke spaja se na posrednika koji je upisan u torrent datoteci, te klijent u kratkom vremenu povratno prima listu ostalih klijenata koji trenutno dohvaćaju dijelove datoteke. Klijent počinje primati dijelove od ostalih klijenata, a takva grupa klijenata koja razmjenjuje datoteku, naziva se roj (engl. swarm). Kada novi klijent pristupi roju razmjenjuje se sama datoteka bez spajanja na inicijalni izvor, no ako se roj sastoji samo od inicijalnog izvora tada potražuje željene datoteke direktno od njega. Način slanja i primanja dijelova je također važan zbog samog opterećenja i dostupnosti pa se tako dijelovi datoteke dohvaćaju nasumično, što je moguće samo ako klijenti posjeduju različite dijelove datoteke. Učinkovitost raspodjele ovisi i o tome sa kime će klijent

razmjenjivati podatke tj. najčešće se odabire razmjena sa onim klijentima koji također posjeduju dijelove datoteke pa se odvija konstantna razmjena, dok novi klijent koji se priključi roju ne može primati nikakve dijelove jer ne posjeduje nikakve dijelove za razmjenu. Jedan od problema je da dva klijenta ne razmjenjuju dijelove zato što niti jedna strana neće prva pokrenuti komunikaciju. Da bi se sve navedeno izbjeglo Bittorrent klijenti koriste mehanizam "optimistično smanjivanje zagušenosti" (eng "optimistic unchoking") koji koristi dio svoje širine pojasa kako bi nasumično odabranim klijentima slao dijelove datoteka, a sve u nadi da će otkriti kvalitetnije partnere za razmjenu [3].

Type	Name (Order by: Uploaded, Size, ULed by, SE, LE) View: Single / Double	SE	LE
Applications (UNIX)	Ubuntu 14.10 desktop x64 Uploaded 10-24 2014, Size 1.08 GiB, ULed by *Anonymous*	128	5
Applications (UNIX)	Ubuntu 16.04.1 LTS Desktop 64-bit Uploaded 08-06 00:00, Size 1.41 GiB, ULed by SeuPirate	48	7
Applications (Other OS)	ubuntu-16.04-desktop-amd64.iso Uploaded 04-22 18:34, Size 1.38 GiB, ULed by *Anonymous*	33	1
Applications (UNIX)	Ubuntu 16.04.1 LTS Desktop 32-bit Uploaded 08-06 00:03, Size 1.43 GiB, ULed by SeuPirate	20	3
Video (Other)	Udemy - Ubuntu Linux Server Troubleshooting Uploaded 08-28 2015, Size 1.37 GiB, ULed by The_Abee	19	5
Other (E-books)	Ubuntu Linux Toolbox 1000+ Commands for Ubuntu and Debian Power Uploaded 12-24 2013, Size 2.49 MiB, ULed by 420weedman	14	0
Other (Other)	Udemy - Ubuntu Linux - Go from Beginner to Power User Uploaded 04-25 19:39, Size 2.43 GiB, ULed by Horisarte	14	5
Applications (UNIX)	Ubuntu Ultimate 1.4 DVD (eng) by http://bestzooom. Uploaded 11-17 2008, Size 1.94 GiB, ULed by dark240293	13	3
Other (E-books)	Beginning Ubuntu Linux - From Novice To Professional[Ebook][ENG- Uploaded 02-14 2010, Size 24.35 MiB, ULed by *Anonymous*	10	1
Applications (UNIX)	ubuntu-13.04-desktop-i386.iso Uploaded 04-25 2013, Size 794 MiB, ULed by markuzmx	10	1
Other (E-books)	The Ubuntu Book 1th Edition 2016 [DeLUXAS] Uploaded 05-02 00:30, Size 16.66 MiB, ULed by *Anonymous*	8	0
Applications (UNIX)	Ubuntu 15.04 Desktop i386, [Iso - MultiLang] [TNTVillage] Uploaded 05-05 2015, Size 1.11 GiB, ULed by mykons	7	0
Other (E-books)	The Official Ubuntu Server Book 3rd Edition(2013)pdf Uploaded 11-03 2014, Size 19.32 MiB, ULed by eboneezer	6	0
Applications (UNIX)	Ubuntu 15.04 Desktop Amd64, [Iso - MultiLang] [TNTVillage] Uploaded 05-05 2015, Size 1.07 GiB, ULed by mykons	6	0
Applications	Ubuntu 14.10 i386 (Desktop ISO)	5	1

Sl. 3.4 Dohvaćanje torrent-a

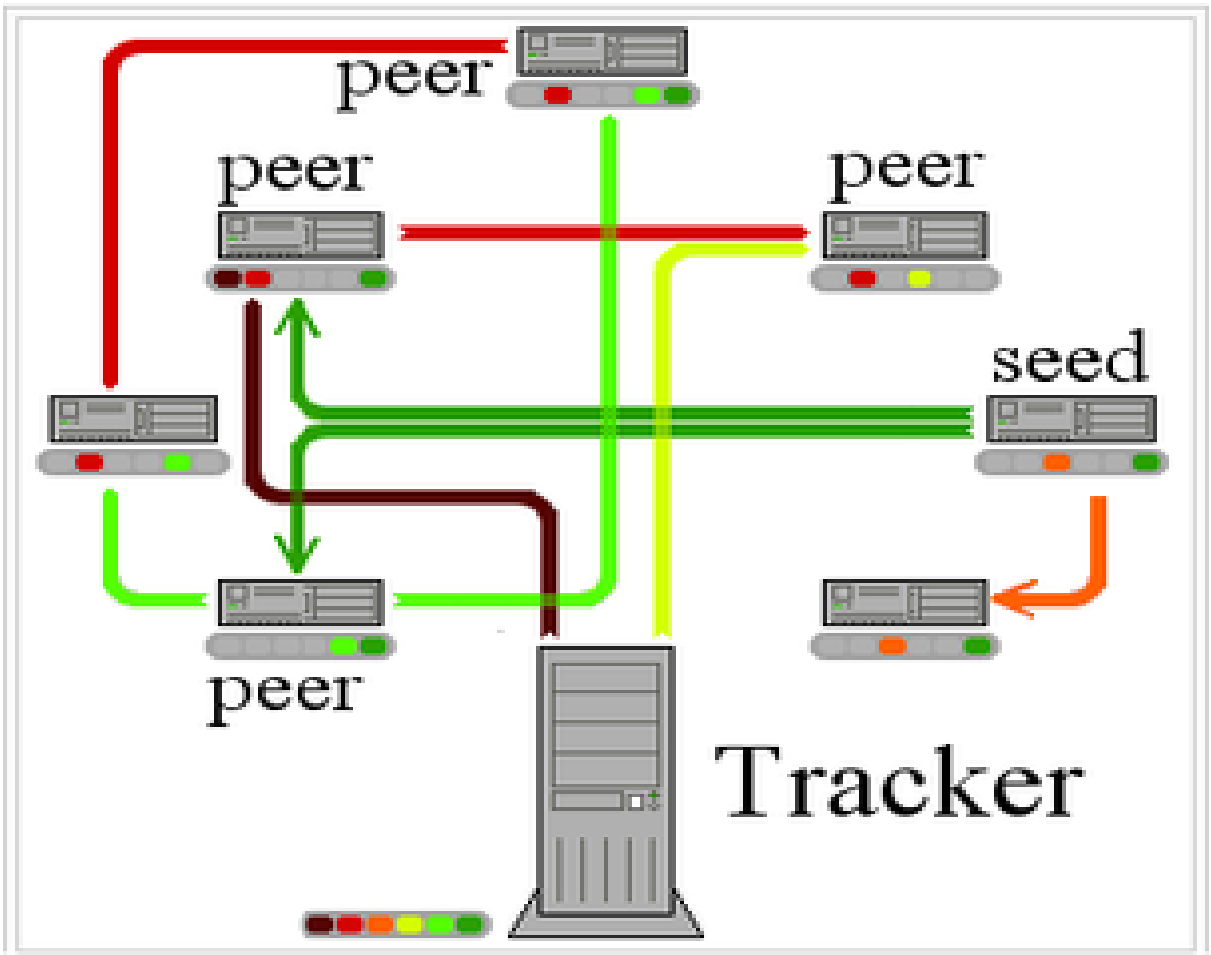


Sl. 3.5 Dijeljenje datoteke

3.4 Implementacija BitTorrent protokola

Uzme se nekakav model poslužitelja koji ima za odgovornost brinuti o detaljima datoteka koje određeni aktivni klijent posjeduje, uz to mora imati pohranjene adrese i vrata klijenata. Poslužitelj također mora biti u mogućnosti odgovarati klijentima na njihove upite. Kada klijent u konačnici pošalje upit za određenom datotekom koju želi dohvatiti poslužitelj prihvati isti i provjerava ga. Ako klijent kao upit pošalje samo ime datoteke, pretražuje se lista svih datoteka i sve što odgovara sprema se u listu peer_list koju kasnije prepisuje u strukturu peers koju je moguće prenijeti preko mreže. Kada klijent pošalje upit vezan samo za detalje oko datoteke problem nastaje jer određene ključne riječi u opisu mogu vratiti više različitih datoteka. Poslužitelj na sve to odgovara sa svim detaljima koje je pronašao a korisnik odabire koju točno datoteku želi. Pretraga se ponavlja sa istim detaljima koje je korisnik odabrao te se nakon pronalaska datoteke šalje odgovor klijentu sa popisima adresa i portova odgovarajućih klijenata. Drugi dio je pak vezan za implementaciju modela klijenta. Klijent mora biti u mogućnosti lokalno pretražiti torrent datoteku kako bi poslao informacije poslužitelju, a da bi poslužitelj

obradio njegov upit klijent mora posjedovati barem jednu datoteku za dijeljenje. Nakon što je klijent pronašao dijeljene datoteke šalje ih poslužitelju i tada može zatražiti datoteku, a odgovor se prividno dijela na dva dijela. Dio koji služi za obradu klijentskih zahtjeva i dio koji služi da se ista datoteka dohvati. Dio koji ima ulogu dohvaćanja slijedno spaja klijente koje je primio u odgovoru i traži sve one dijelove datoteke koji mu nedostaju. Nakon svih pronađenih klijenata datoteka može ali i ne mora biti potpuno prenesena. Ako nedostaju dijelovi klijent se nakon nekog vremena može ponovno spojiti na poslužitelj i skinuti dijelove koji mu nedostaju. Nakon završenog prijenosa klijentski dio je završen a poslužiteljski dio nastavlja obradu sve do izlaska iz programa [4].

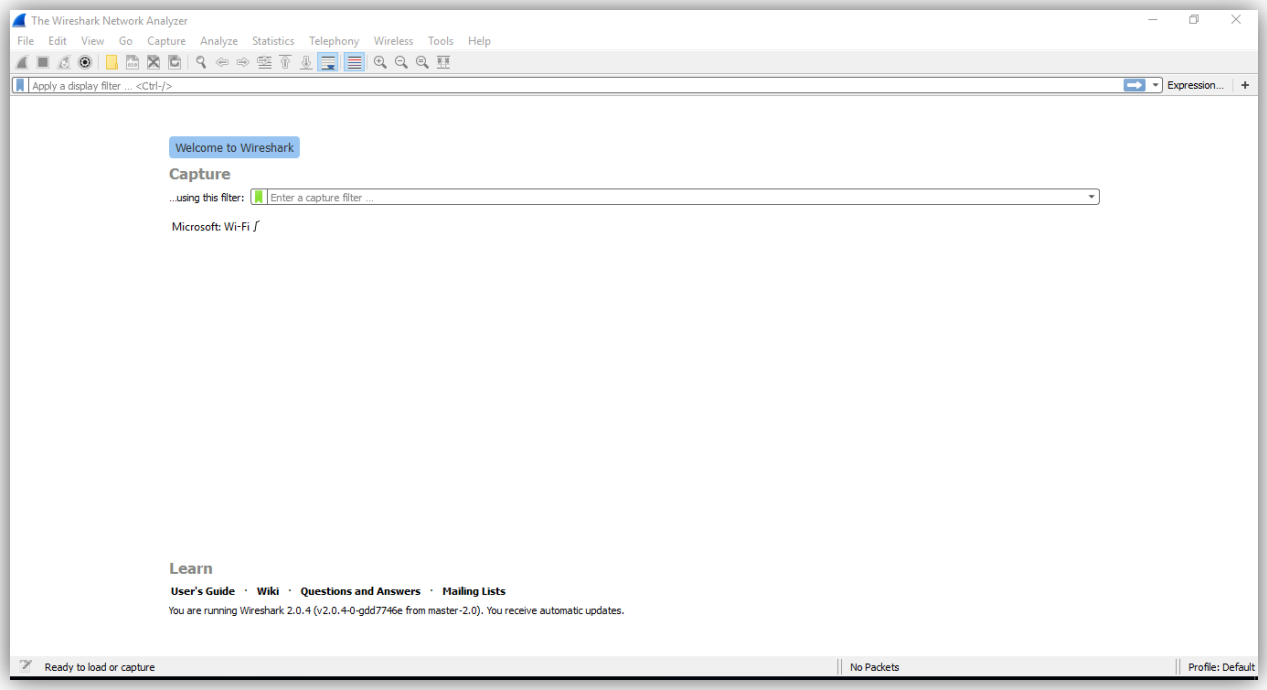


Sl. 3.6 Grafički prikaz rada Bittorent protokola

4. ANALIZA BITTORRENT PROTOKOLA POMOĆU WIRESHARK-a I UTORRENT KLIJENTA

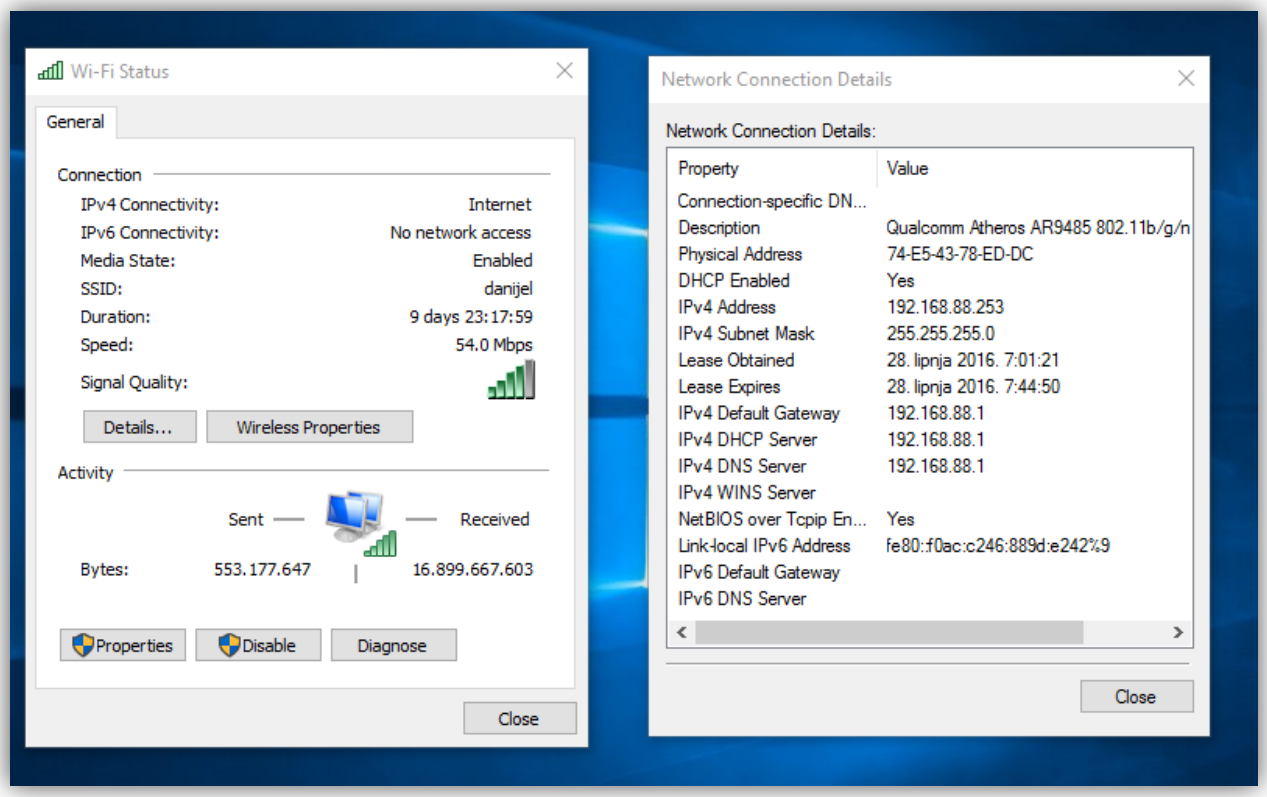
Program Wireshark često se u praksi koristi za hvatanje, filtriranje, izvoz i uvoz paketa. Wireshark u odnosu na ostale alate ima grafičko sučelje što pojednostavljuje korištenje istoga. Glavno obilježje Wiresharka je svakako hvatanje mrežnih paketa tj. "osluškivanje" mreže. Cilj je prikazati kako se zatražene torrent datoteke skidaju i to pratimo preko utorrent klijenta i njegovih ugrađenih alata za analizu. Uz to prikazana je i analiza kroz Wireshark kao samostalni program koji ima veću mogućnost dodatnih opcija tijekom pretrage i analize pojedinih podataka [5].

Za početak pokreće se Wireshark prema slici 4.1 i dobiva se početno grafičko sučelje u kojem se odabire što se želi pratiti i analizirati tj. što se želi filtrirati.



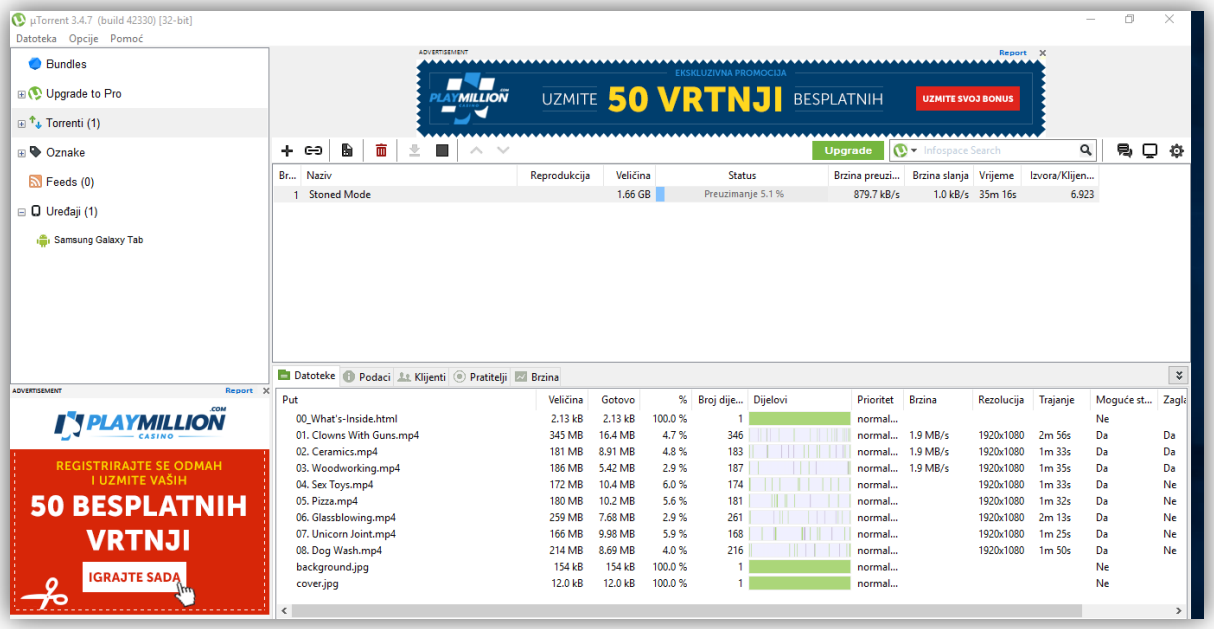
Sl. 4.1 Wireshark

Prije svega mora se pronaći IP adresa vašeg računala kako bi ju izdvojili i vidjeli sa kojim se to IP adresama komunicira. Važno je odrediti vlastitu IP adresu kako bi se orijentirali između ostalih IP adresa koje će Wireshark prikazati.



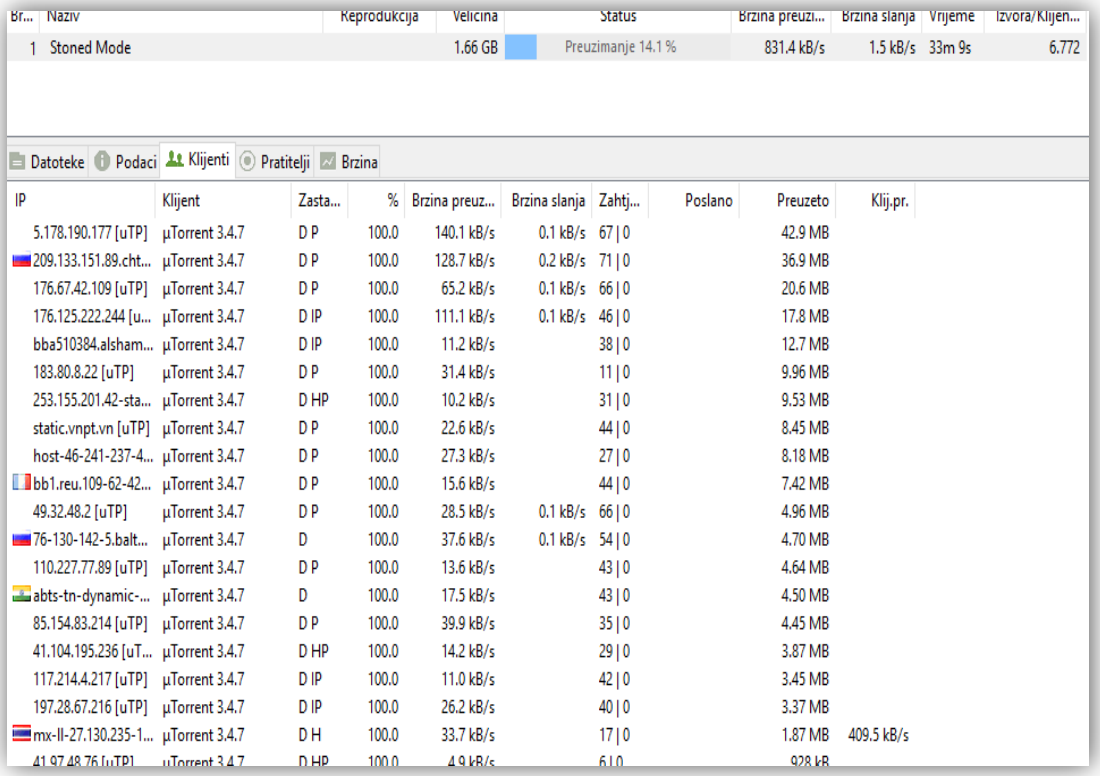
Sl. 4.2 Podaci sa računala

Jednom kada doznate sve podatke o adresama vidljivo prema slici 4.2 možete pokrenuti određenu torrent datoteku pomoću utorrent klijenta. Pokretanjem se mogu vidjeti osnovne stvari poput brzine skidanja datoteke, što sve ona sadrži, veličinu, download/upload brzinu, prosječno vrijeme skidanja itd. (Sl. 4.3).



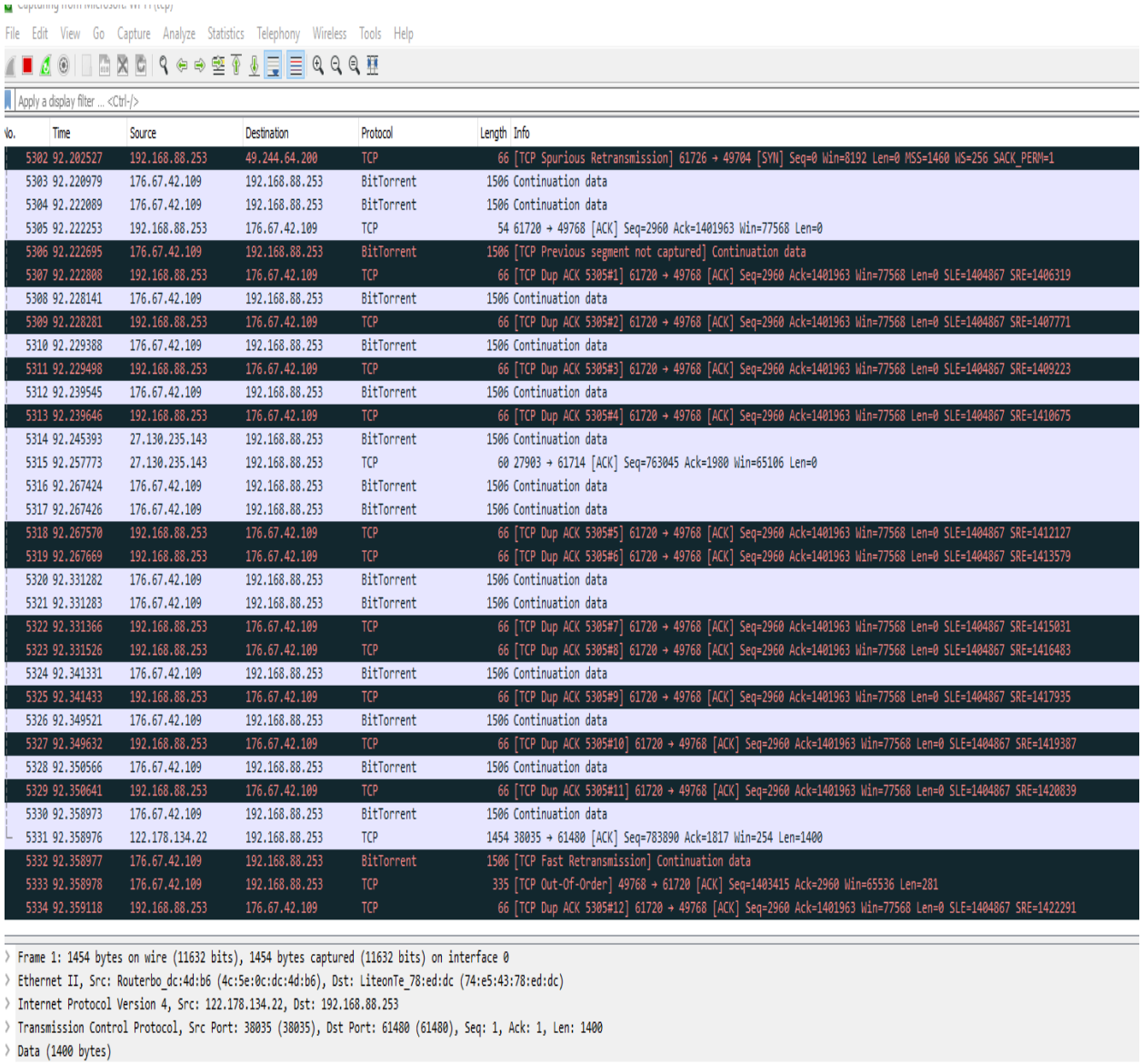
Sl. 4.3 Skidanje datoteke Stone mode

Preko utorrent klijenta moguće je provjeriti i određene podatke od kojih klijenata se prikupljaju dijelovi datoteke i to pod opcijom "klijenti". Vidljiva je lista klijenata kao i brzina preuzimanja od pojedinog klijenta, u kojem te koliko je do toga trenutka i koliko preuzeto (Sl. 4.4).



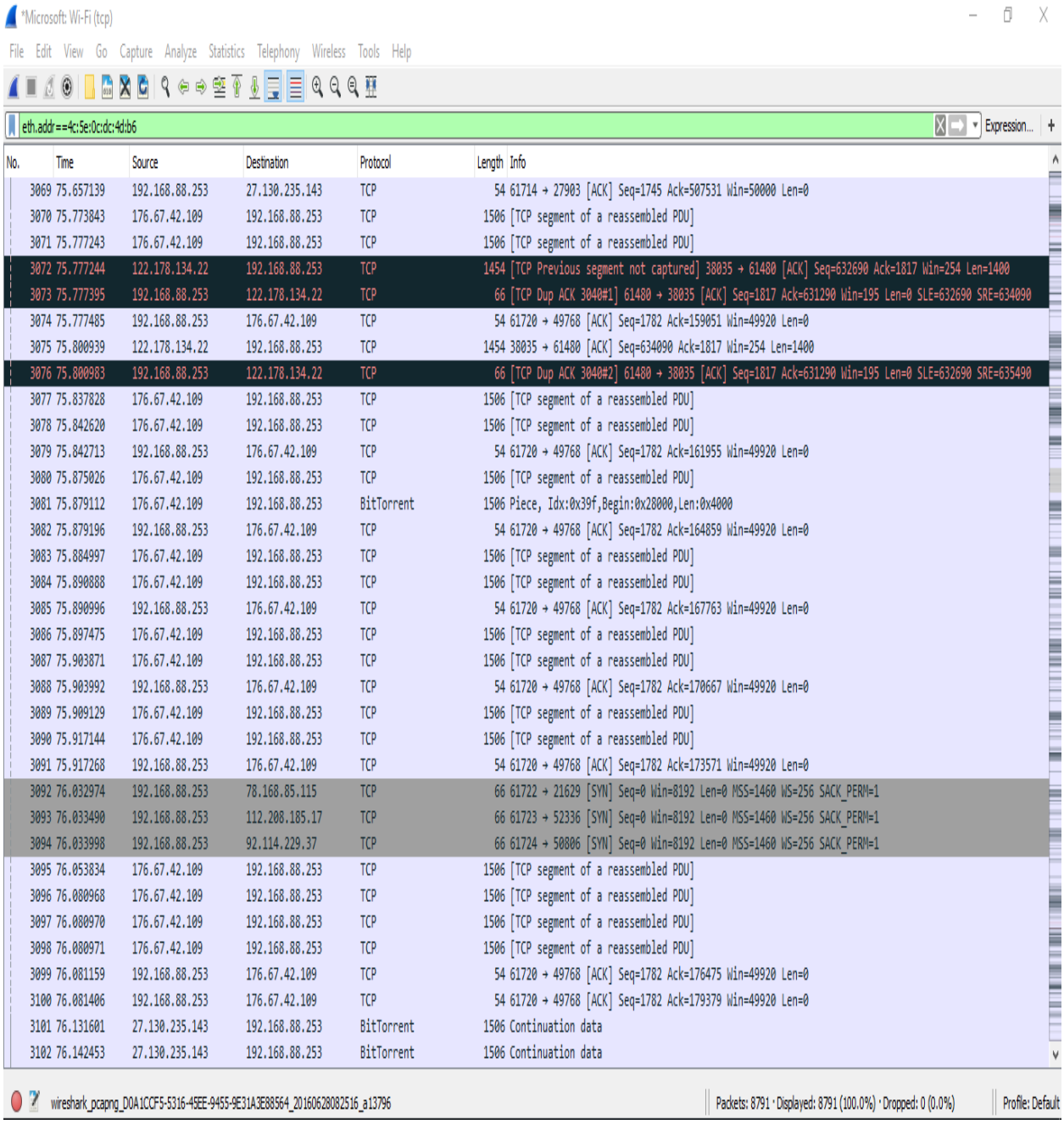
Sl. 4.4 Popis klijenata

Sada kada se datoteka pokrenula i uredno se skida na računalo možemo se vratiti u Wireshark i početi hvatati pakete koji se razmjenjuju te izvršiti analizu uhvaćenog. Kada se pokrene program vidi se gomila podataka koji popunjavaju listu i bilježe sve što se zatražilo već u prvim sekundama (Sl.4.5).



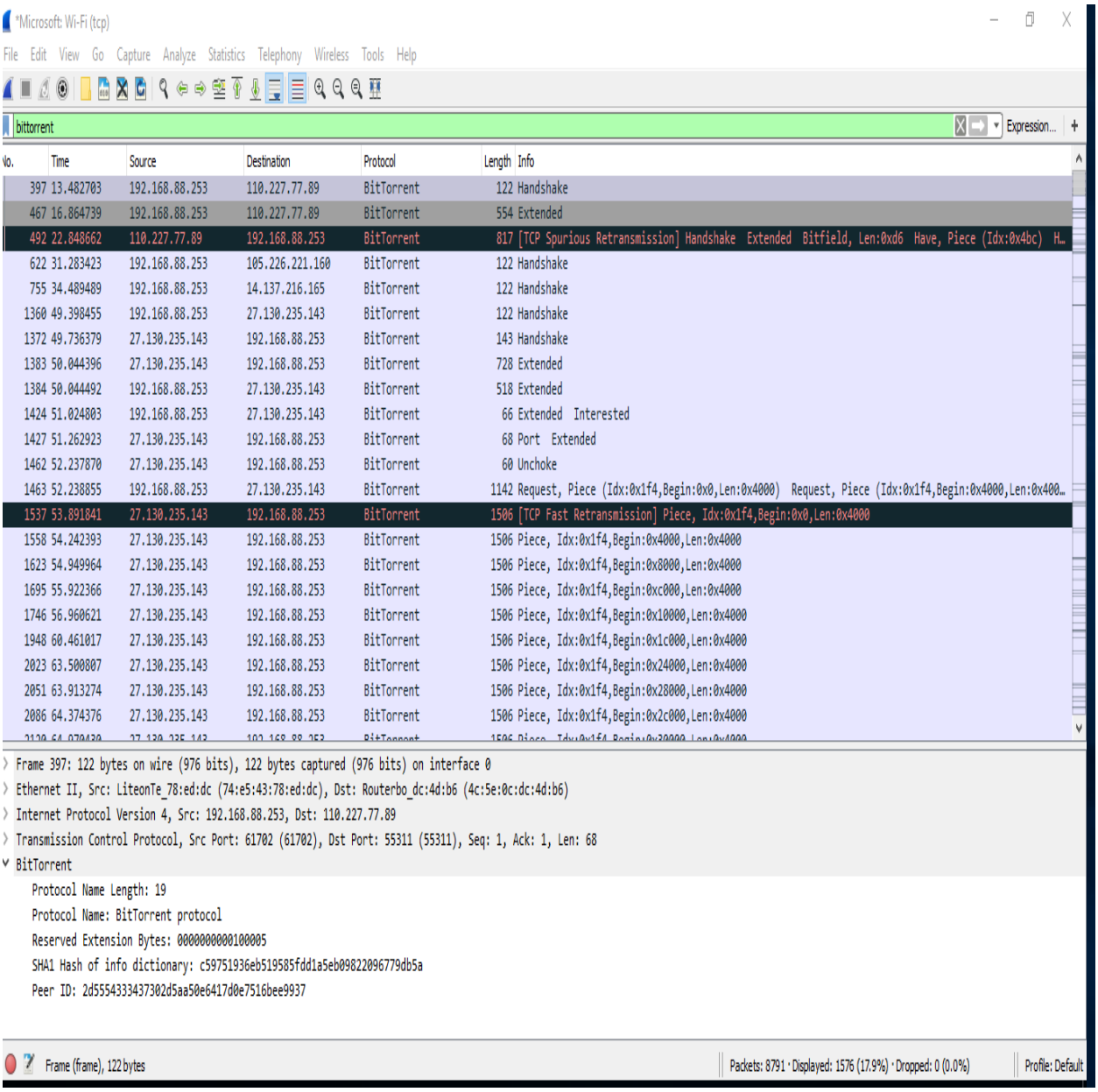
Sl. 4.5 Hvatanje podataka

Kako bi izdvojili samo svoju adresu i vidjeli sa kime sve komuniciramo na alatnoj traci nalazi se "Statistics" i odabere se "Endpoints. Adresa koja je promatrana je 192.168.88.253. Nakon toga prikazan je filtar po adresi sa slijedećim rezultatima (Sl. 4.6).



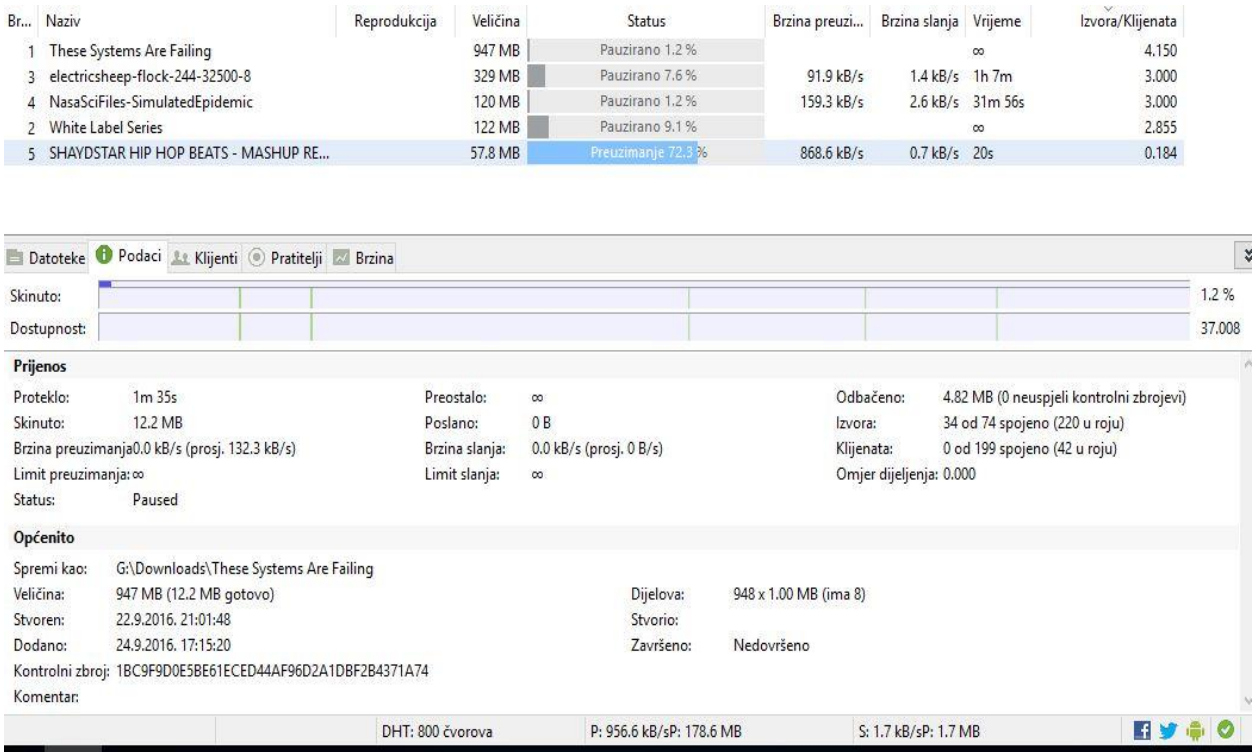
Sl. 4.6. Filtriranje po adresi

Može se posebno izdvojiti BiTorrent protokol upisivanjem u filter "Bittorrent" i dobiva se prikaz na listi vezan samo uz navedeni protokol. Ispod liste nalazi se prozor sa analizom sadržaja paketa u kojem su dostupne nekakve osnovne informacije (Sl 4.7).



Sl. 4.7 Filtriranje po protokolu

Nakon prolaska kroz Wireshark pokrenut će se nekoliko torrenata sa različitim sadržajem, veličinom, omjerom seedera/leachera itd., kako bi se na temelju različitih kriterija prikazalo kako i što se sve odvija kod krajnjeg korisnika.



Sl 4.7 Pokretanje nekoliko torrent-a

Postavlja se nekoliko torrent datoteka na preuzimanje pronađenih sa različitih web stranica, te se prikupljaju pojedinačni podatci na temelju kojih će se prikazat statistika svake pojedine torrent datoteke prema [6].

U prvom dijelu tablice nalazi se datoteka **"SHAYDSTAR HIP HOP BEATS…"** vidljivo glazbenog sadržaja sa slijedećim podatcima, te dalje slijede ostale datoteke.

Naziv	**"SHAYDSTAR HIP HOP BEATS…"**
Veličina	57.8 MB
Prosječna brzina download-a	132.3 Kb/s
Prosječna brzina upload-a	0.3 Kb/s
Odbačeno	6.14 MB
Izvora	34 od 74 spojeno (220 u roju)
Klijenata	0 od 199 spojeno (42 u roju)
Ukupno vrijeme preuzimanja	3m 41s
Naziv	**"White Label Series"**
Veličina	122 MB
Prosječna brzina download-a	512.0 Kb/s
Prosječna brzina upload-a	0.3 Kb/s
Odbačeno	21.5 MB
Izvora	13 od 39 spojeno (4101 u roju)
Klijenata	0 od 137 spojeno (4 u roju)
Ukupno vrijeme preuzimanja	4m 24s

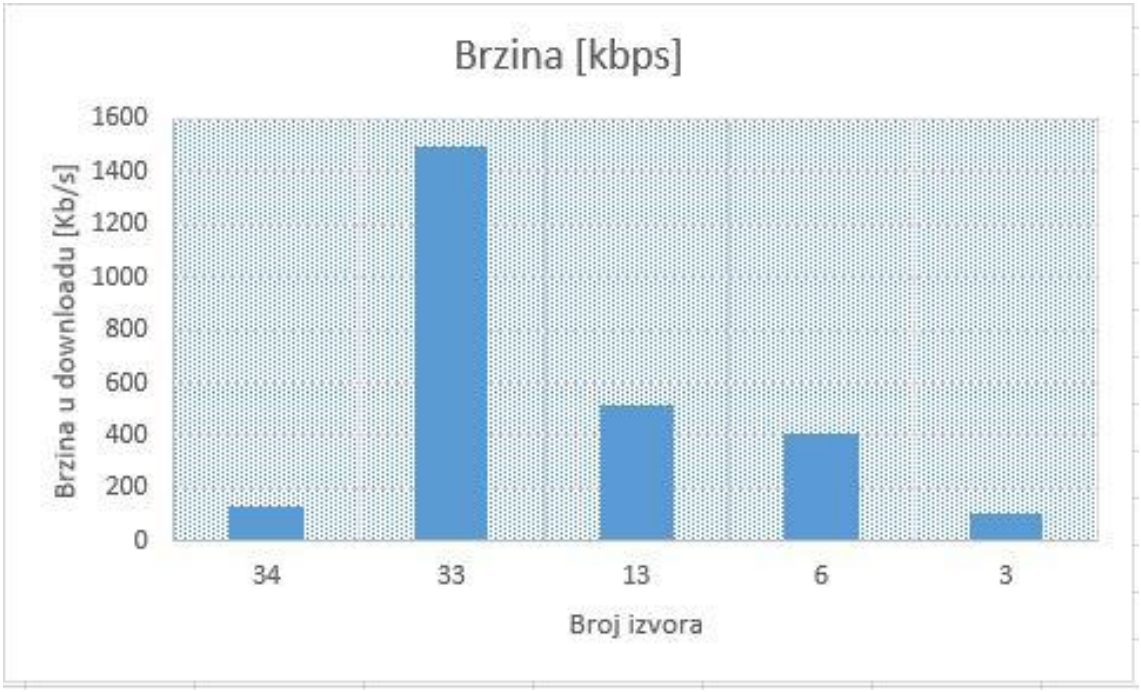
Naziv	**''These Systems Are Failing''**
Veličina	947 MB
Prosječna brzina download-a	1.5 MB/s
Prosječna brzina upload-a	6.3 Kb/s
Odbačeno	7.05 MB
Izvora	33 od 77 spojeno (220 u roju)
Klijenata	0 od 200 spojeno (42 u roju)
Ukupno vrijeme preuzimanja	10m 6s
Naziv	**''Atlantis (Demo Taped Remix''**
Veličina	8.30 MB
Prosječna brzina download-a	404.9 Kb/s
Prosječna brzina upload-a	0.3 Kb/s
Odbačeno	1.52 MB
Izvora	6 od 8 spojeno (3014 u roju)
Klijenata	0 od 200 spojeno (9 u roju)
Ukupno vrijeme preuzimanja	35s
Naziv	**''electrictsheep-flock-244-32500-8''**
Veličina	329 MB
Prosječna brzina download-a	102.9 Kb/s
Prosječna brzina upload-a	0.2 Kb/s
Odbačeno	114 MB
Izvora	3 od 3 spojeno (0 u roju)
Klijenata	0 od 1 spojeno (1 u roju)
Ukupno vrijeme preuzimanja	55m 35s

Tab. 4.1 Podatci preuzetih datoteka

Iz priložene tablice 4.1 vidljivo je kako se torrent datoteke preuzimaju uz različite faktore koji utječu za koje će se vrijeme preuzeti data datoteka. Vidljiv je jasan zaključak da omjer seedera/leachera najviše utječe na ukupno vrijeme skidanja datoteke, dakle bolje je imati što više seeder-a a što manje leacher-a. Nadalje ukoliko skidamo više datoteka odjednom poželjno je da internetska veza ima što veću propusnost, te na kraju same postavke programa preko kojeg skidamo datoteke u kojem se također može regulirati brzina download-a i upload-a.

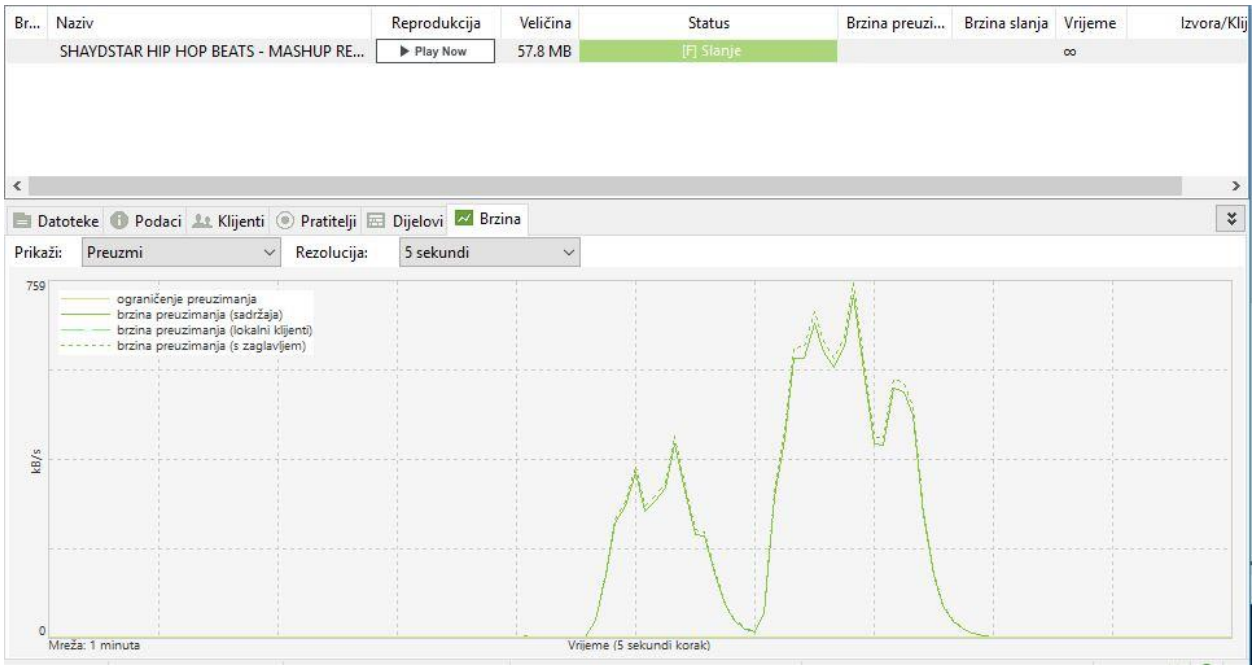
Sl. 4.8 Brzina preuzimanja svih torrent datoteka

Prema slici 4.8 vidljivo je da brzina preuzimanja oscilira tijekom preuzimanja svih 5 datoteka te da se konstantno mijenja ovisno o svakoj pojedinoj datoteci. Nadalje, prikazano je prema slici 4.9 kako izvori utječu na prosječnu brzinu preuzimanja datoteke.



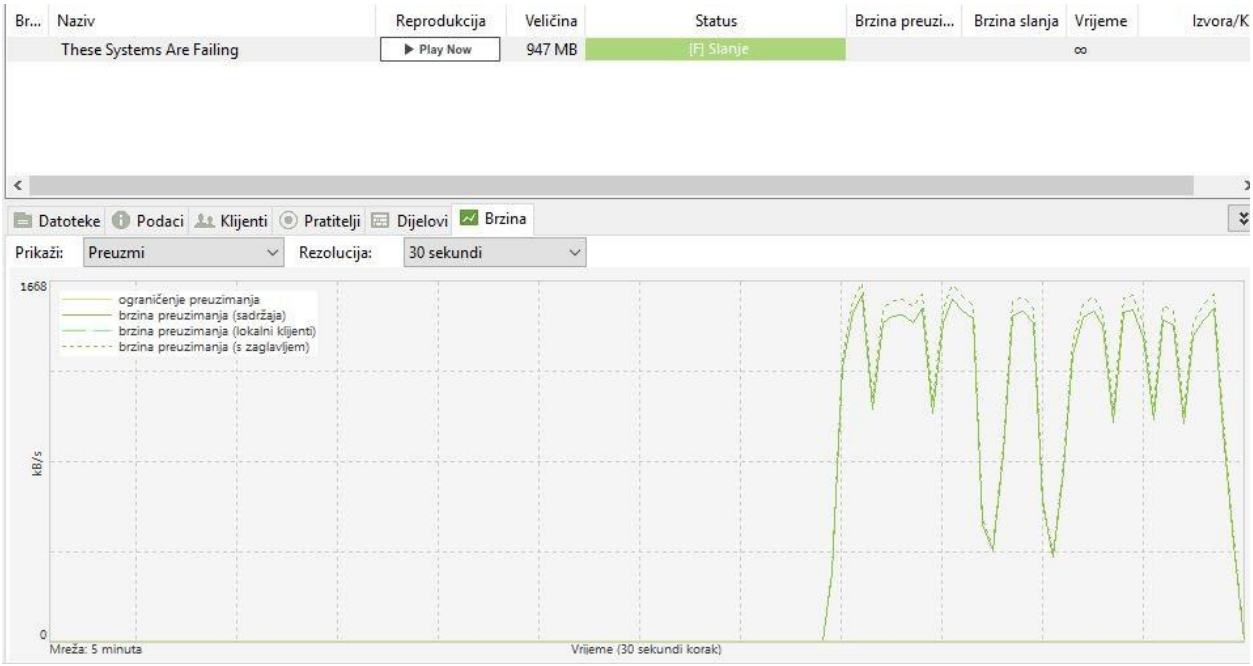
Sl. 4.9 Utjecaj izvora na brzinu preuzimanja

Prema slici 4.9 vidimo ovisnost broja izvora o prosječnoj brzini preuzimanja torrent datoteke, što je više izvora sama brzina raste te se krajnje vrijeme za preuzimanje datoteke smanjuje. No kako je vidljivo pojedine datoteke tijekom preuzimanja ili izgube izvore ili se poveća broj klijenata pa samim time pada prosječna brzina preuzimanja datoteke, vidljivo kod prvog primjera "SHAYDSTAR HIP HOP BEATS" glazbene datoteke koja tijekom preuzimanja dobiva sve više klijenta i samim time prosječna brzina je u padu jer se broj izvora nije povećavao, dakle imamo 34 izvora sa prosječnom brzinom preuzimanja od 132,3 Kb/s.



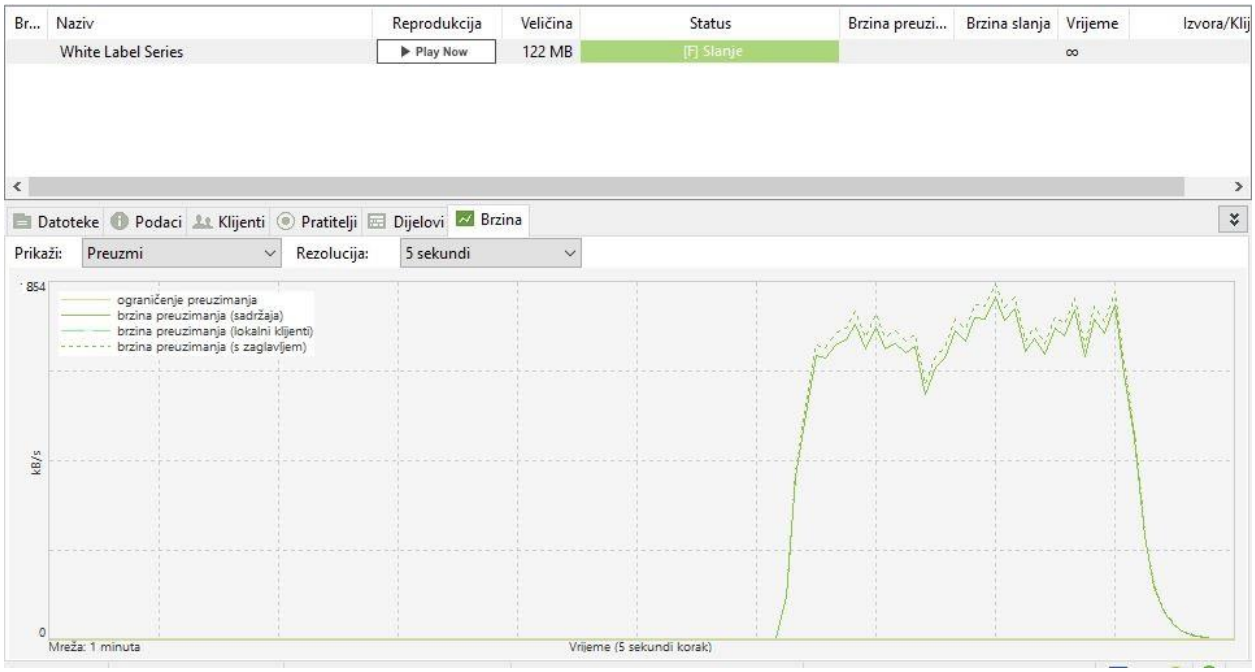
Sl. 4.10 Brzina tijekom preuzimanja "SHAYDSTAR HIP HOP …"datoteke

Kod preuzimanja datoteka prema slici 4.10 nije rijedak slučaj da u jednom trenutku imamo veliku brzinu kojom preuzimamo datoteku dok u drugom ona naglo opada zbog promjene omjera izvora i klijenata, tj., povećao se broj klijenata tijekom preuzimanja dok je broj izvora ostao isti., te se samim time i mijenja konačno vrijeme, u ovom slučaju vrijeme preuzimanja se povećava.



Sl. 4.11 Brzina tijekom preuzimanja "These Systems Are Failing" datoteke

Nadalje slijedi datoteka **''These Systems Are Failing''** sa 33 izvora i prosječnom brzinom preuzimanja od 1500 Kb/s prema tablici 4.1, što je nekoliko puta veće od prethodne datoteke. Vidljivo je da se broj klijenata nije povećavao i samim time osigurano je kraće vrijeme preuzimanja datoteke vidljivo prema slici 4.11 gdje brzina preuzimanja oscilira između 1300 Kb/s i 1700 Kb/s što je u prosjeku nakon preuzimanja datoteke iznosilo oko 1500 Kb/s i samim time postiglo najveću brzinu preuzimanja u odnosu na ostale datoteke iz tablice 4.1.

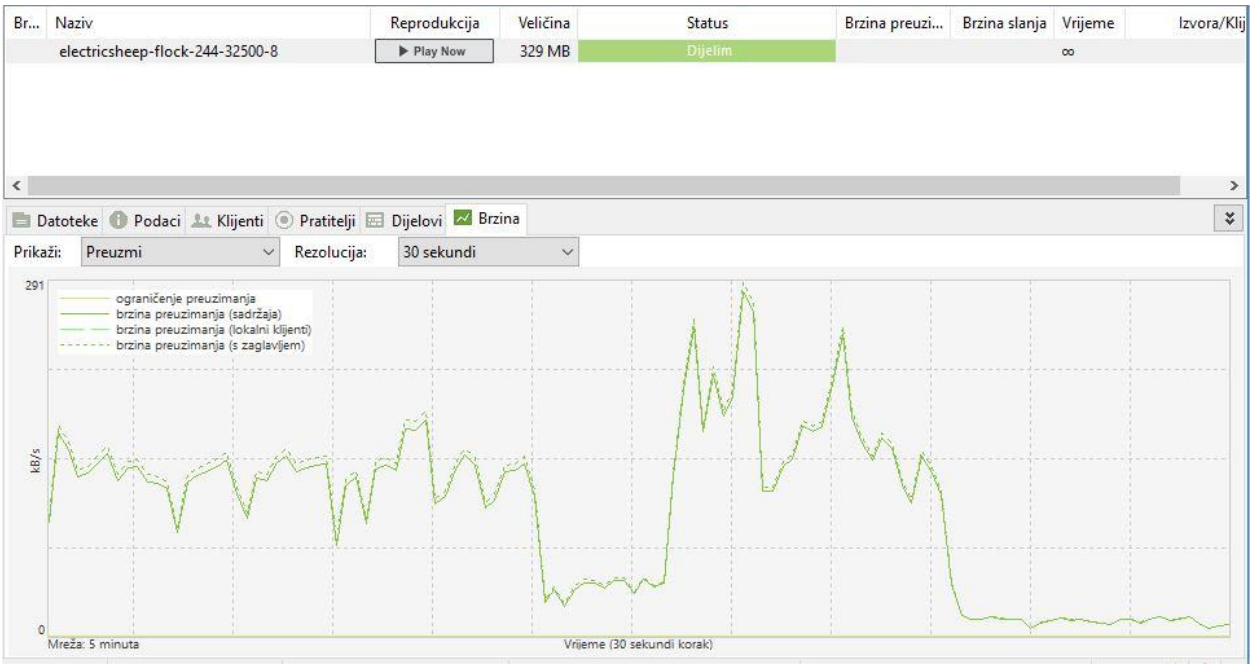


Sl. 4.12 Brzina tijekom preuzimanja "White Label Series" datoteke

Datoteka **''White Label Series''** sa svojih 13 izvora uspijeva dostići prosječnu brzinu preuzimanja od 512 Kb/s prema tablici 4.1, te samim time pokazuje da u odnosu na datoteku **''SHAYDSTAR HIP HOP BEATS''**, koja je gotovo upola manja i koja ima 34 izvora, uspijeva preuzeti znatno brže prema slici 4.12, jer se broj klijenata nije znatno povećavao tijekom preuzimanja.

Sl. 4.13 Brzina tijekom preuzimanja "Atlantis (Demo Taped Remix)" datoteke

Na kraju imamo dvije datoteke sa manjim brojem izvora ali različitim veličinama, prema tablici 4.1, sa 6 izvora **''Atlantis (Demo Taped Remix)''** i prosječnom brzinom preuzimanja od 404,9 Kb/s te s veličinom od samo 8,3 MB preuzima za samo 35 sekundi prema slici 4.13, te na kraju dolazi datoteka **''electrictsheep-flock-244-32500-8''** koja prema tablici 4.1 ima samo 3 izvora i kao takva dostiže prosječnu brzinu preuzimanja od 102.9 Kb/s ali uz napomenu da je tijekom prijenosa podataka čak 114 MB odbačeno kao neuspjeli prijenos.



Sl. 4.14 Brzina tijekom preuzimanja "electrictsheep-flock-244-32500-8" datoteke

Prema slici 4.14 vidljivo je da se datoteka **''electrictsheep-flock-244-32500-8''** vremenski gledano najduže preuzimala u odnosu na ostale datoteke, naravno uzimajući u obzir da raspolaže samo sa 3 izvora. Također vidljivo je da je 114 MB odbačeno tijekom preuzimanja što je dodatno produžilo vremenski period preuzimanja. Navedeno govori da datoteke sa malim brojem izvora najčešće imaju male brzine tijekom preuzimanja, uz napomenu da takve datoteke ponekad "zakažu" tijekom preuzimanja tj. da se brzina smanji do te granice da se datoteka može skidati satima ili čak danima, a moguće je da se uopće ne uspiju preuzeti do kraja.

5. ZAKLJUČAK

Od dana kada su se pojavile p2p mreže dolazi do velikog preokreta na internetu. Korisnici koji su prije samo pretraživali internet, čitali poštu i novine, a danas su aktivni sudionici u velikoj razmjeni podataka kako svojih podataka tako i preuzimanju drugih. Jedna od prednosti je dostupnost velikog broja podataka preko velikog broja klijenata, svaki klijent koji preuzme nekakav sadržaj ujedno postaje i izvor istoga te se dostupnost određenog sadržaja povećava proporcionalno povećanju klijenata. Imamo sve više izvora što rezultira bržem pristupu podatcima , a samim time i većim brzinama prijenosa podataka. Ukoliko jedan od klijenata zakaže prijenos podataka se nastavlja preko ostalih klijenata te samim time se p2p mreža nastavlja bez ikakvih posljedica. Međusobno povezivanje i razmjena, te velik broj raznovrsnog dostupnog sadržaja iz dana u dan osigurava p2p mrežama bolju i sigurniju budućnost. Popularnost torrenata pokazuje koliko korisnici sve više pristupaju razmjeni resursa i potragom za što većim brzinama prijenosa, što postavlja pred telekomunikacijske operatere sve veće izazove. Glavni izazov je upitna legalnost resursa koji se razmjenjuju u p2p mrežama jer nema mogućnosti kontrole takvih sadržaja, što najčešće rezultira povredom autorskih prava. Također je problem sa nepoznatim izvorima koji mogu sadržavati opasne viruse i tako zaraziti velik broj računala na koje se preuzima sadržaj. Realno gledano, ako se u budućnosti riješi problematika legalnosti sadržaja u p2p mrežama možemo očekivati i promjene u samoj arhitekturi internet mreža.

LITERATURA

[1] Peer-to-peer-mreže-CARNet Cert, pdf dokument:

http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2009-11-282.pdf

[2] Seminarski rad, doc. dokument:

www.mathos.unios.hr/~isimic1/seminari/Seminar(**p2p**-tcp-udp).doc

[3] Završni rad, Hrvoje Kostić 2008.g., pdf dokument:

https://bib.irb.hr/datoteka/409255.Hrvoje_Kostic_-_Zavrsni_rad.pdf

[4] Understanding of BitTorrent Protocol, pdf dokument:

https://www.google.hr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0ahUKEwi0nJfuwL_PAhUkJ8AKHXDjAgIQFghsMAk&url=http%3A%2F%2Fdandylife.net%2Fblog%2Fwp-content%2Fuploads%2F2013%2F07%2FBitTorrent-Protocol.pdf&usg=AFQjCNEx8EIIiwypCufF5UYxUE88-1OGPQ&sig2=SsWypIgXdvUFCt8cDAqemQ

[5] Analiza alata Wireshark-CARNet CERT, pdf dokument:

http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-09-312.pdf

[6] uTorrent i njegova upotreba, html:

http://www.racunalniska-pomoc.si/hr/utorrent-in-njegova-uporaba/

SAŽETAK: Analiza BitTorrent protokola pomoću analizatora mrežnog prometa

Peer-to-peer (p2p) koristi koncept umrežavanja računala u kojem nema servera tj. poslužitelja, svako je računalo i server i klijent. U takvoj mreži korisnici razmjenjuju datoteke međusobno i to će se prikazati na konkretnim primjerima, u našem primjeru preko uTorrent klijenta. Prolaze se osnovne stvari po pitanju p2p mreža, od podjele do nekih osnovnih karakteristika. Govori se o BiTtorrent protokolu, obrađuje se princip rada i daljnja implementacija p2p mreža. U ovom završnom radu koristi se Wireshark alat za praćenje i analizu mrežnih podataka, posebice BitTorrent protokola.

Ključne riječi: poslužitelj, klijent, torrent, p2p, BitTorrent, uTorrent, WireShark

ABSTRACT: BitTorrent protocol analysis using network traffic analyzer

Peer-to-peer (P2P) uses the concept of networking computers in which has no server. Each computer is a server and a client. In such network, users exchange files with each other and this will show through concrete examples, in our example over the uTorrent client. We pass the basic things in terms of P2P networks, from distribution to some basic characteristics. We are talking about the BitTorrent protocol, process operating principle and further implementation of P2P networks. In this final work we use Wireshark tool for monitoring and analyzing network data, in particular the BitTorrent protocol.

Keywords : server, client, torrent, P2P, BitTorrent, uTorrent, WireShark.

Ž I V O T O P I S

Danijel Primorac rođen je 08. veljače 1991. u Osijeku s prebivalištem u Belišću na adresi Kralja Tomislava 211. Završava osnovnoškolsko obrazovanje u Osnovnoj školi Ivana Kukuljevića u Belišću te srednjoškolsko obrazovanje u Srednjoj školi Valpovo, smjer opća gimnazija. Tijekom osnovne i srednje škole bio je član nogometnog kluba NK Belišće i član Streljačkog društva Stjepan Petnjarić Belišće. Upisuje Elektrotehnički fakultet u Osijeku 2011./2012. godine, stručni studij smjera informatike. Tijekom studija se zapošljava u Hrvatskom Telekomu u sektoru za servis i upravljanje uslugama sa privatnim i poslovnim korisnicima u kojem radi i danas. Po završetku studija trajno se zapošljava u Hrvatskom Telekomu.

_____

Potpis