Analiza programskih alata za logičku provjeru mrežnih protokola

Kos, Dino

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Dino Kos

ANALIZA PROGRAMSKIH ALATA ZA LOGIČKU PROVJERU MREŽNIH PROTOKOLA

ZAVRŠNI RAD

Zagreb, 2017.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 22. ožujka 2017.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Računalne mreže**

ZAVRŠNI ZADATAK br. 3970

Pristupnik: **Dino Kos (0135224536)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza programskih alata za logičku provjeru mrežnih protokola**

Opis zadatka:

Objasniti funkciju i značaj mrežnih protokola te prikazati klasifikaciju protokola u funkciji računalnih mreža. Objasniti ulogu logičke provjere mrežnih protokola. Pregledno prikazati programske alate i sustave za analizu mrežnih protokola. Napraviti komparativnu analizu programskih alata za analizu mrežnih protokola.

Zadatak uručen pristupniku: 28. travnja 2017.

Mentor:

doc. dr. sc. Ivan Grgurević

Predsjednik povjerenstva za završni ispit:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA PROGRAMSKIH ALATA ZA LOGIČKU PROVJERU MREŽNIH PROTOKOLA

ANALYSIS OF SOFTWARE TOOLS FOR LOGICAL NETWORK PROTOCOL VERIFICATION

Mentor: doc. dr. sc. Ivan Grgurević

Student: Dino Kos

JMBAG: 0135224536

Zagreb, rujan 2017.

ANALIZA PROGRAMSKIH ALATA ZA LOGIČKU PROVJERU MREŽNIH PROTOKOLA

SAŽETAK

Logička provjera mrežnih protokola prikazuje i opisuje koji su se protokoli koristili na mreži za vrijeme obavljanja određenih funkcija. U završnom radu detaljno je prikazana analiza i provjera mrežnih protokola te je napravljeno skeniranje mrežnog sučelja. Protokoli su analizirani u odabranim programskim alatima te su na temelju dobivenih rezultata prikazane pripadajuće karakteristike. Pomoću programskih alata ustanovljeno je koji se protokoli koriste na kojem dijelu mreže te je li njihova upotreba pouzdana ili nije. Programski alati su međusobno uspoređeni prema funkcijama, glavnim značajkama te prednostima i nedostacima.

KLJUČNE RIJEČI: logička provjera mrežnih protokola; mrežno sučelje; skeniranje; analiza

SUMMARY

The logical network protocol verification displays and describes which protocols are used on the network while performing certain functions. In the Bachelor's thesis detailed analysis and testing of network protocols is shown and the network interface scan is made. The protocols are analyzed in selected program tools and based on the results obtained, the relevant characteristics are displayed. The program tools has identified which protocols are used on which part of the network and whether their usage is reliable or not. Program tools are compared to the functions, main features, advantages and disadvantages.

KEYWORDS: logical verification of network protocols; network interface; scanning; analysis

Sadržaj

1. Uvod

Korištenje Interneta danas je svakodnevica velikom broju ljudi. Kao i bilo koji drugi veliki sustav, Internet također ima svoje sastavne dijelove bez kojih ne bi mogao funkcionirati. Među njih spadaju i protokoli koji se prilikom Interneta koriste od čega svaki ima svoju, drugačiju funkciju bilo da se radi o protokolima za prijenos podataka, uspostavu veze, obradu podataka ili sigurnosti mreže. Protokoli su raspoređeni po slojevima kojih ima sedam (7) ako se radi o OSI referentnom modelu ili četiri (4) ako se pak radi o TCP/IP modelu. Cilj završnog rada je provesti analizu programskih alata i sustava za logičku provjeru mrežnih protokola. Također su detaljno obrađeni programski alati kojima se obavlja logička provjera protokola kojom se utvrđuje korištenje protokola na Internetu te se hvataju mrežni paketi koji se prikazuju na korisničkom sučelju na kojem je moguće vidjeti sve važne informacije i detalje o pojedinim paketima i protokolima. Svrha završnog rada je na temelju dobivenih rezultata logičke provjere mrežnih protokola ustanoviti koji se protokoli najviše koriste na pojedinim dijelovima mreže te na temelju njihovih informacija usporediti dobivene rezultate.

Ovaj rad je podijeljen u sedam poglavlja, a to su redom:

1. Uvod,
2. Funkcija i značaj mrežnih protokola,
3. Klasifikacija protokola u funkciji računalnih mreža,
4. Logička provjera mrežnih protokola,
5. Pregled programskih alata i sustava za analizu mrežnih protokola,
6. Komparativna analiza programskih alata i sustava za analizu mrežnih protokola te
7. Zaključak.

Uvodno poglavlje daje osnovnu sliku o radu te definira cilj, svrhu i strukturu rada. U drugom poglavlju opisani su slojevi referentnih modela s pripadajućim protokolima te njihove zadaće, funkcija, značaj te korištenje. U trećem poglavlju su detaljno opisani svi protokoli po slojevima, njihove prednosti i nedostaci te međusobna usporedba nekih sličnih protokola. Nadalje, opisana je logička provjera mrežnih protokola i njezina upotreba te funkcija i zadaće. U petom i šestom poglavlju su obrađeni programski alati koji su korišteni za

logičku provjeru, prikazani su njihovi rezultati, pogreške i problemi koji su prisutni na mreži te je obrađena komparativna analiza pomoću koje je moguće vidjeti koji je alat najpraktičniji za korištenje ovisno o onome što je korisniku u određenom trenutku potrebno. U Zaključku je sažeto sve najbitnije iz prethodnih poglavlja s kratkim osvrtom na rad i buduća istraživanja.

2. Funkcija i značaj mrežnih protokola

Mrežni protokol je skup pravila kojih se računalo mora pridržavati kako bi moglo uspješno komunicirati s drugim računalima u mreži. Mrežni se protokol brine da svi podaci sigurno dođu do odredišnog računala. Mrežni protokoli određuju pravila uspostave veze, prijenos podataka te način prekida veze [27]. Protokoli se nalaze na svakom sloju referentnih OSI i TCP/IP modela. Razlika između ta dva referentna modela je u broju slojeva. OSI[1] (*Open systems interconnection*) model omogućava stvaranje komunikacijskog lanca od proizvoda različitih proizvođača. OSI referentni model je apstraktni model koji služi kao preporuka stručnjacima za razvoj protokola računalnih mreža. Ovaj model pruža važne smjernice u razvoju mrežnih protokola. Mrežni komunikacijski protokol predstavlja skup određenih pravila kao što su prikaz podataka, autorizacija, signalizacija te otkrivanje pogrešaka koja su potrebna da bi se podaci mogli prenijeti preko komunikacijskog kanala. OSI model je podijeljen u sedam slojeva, gdje svaki sloj opisuje skup povezanih funkcija koje omogućuju dio računalnih komunikacija. Ti slojevi prikazuju protok podataka od izvora prema odredištu. Slojevi unutar modela komuniciraju sa slojem ispod i slojem iznad sebe. Između slojeva definirana su sučelja. Gornji protokol ovisi o funkcionalnosti protokola ispod [1]. OSI model olakšava razvoj protokola i komunikacije, a njegovom podjelom na slojeve omogućen je ubrzan razvoj protokola za pojedini sloj. Slojevi OSI modela su fizički, podatkovni, mrežni, prijenosni, sesijski, prezentacijski i aplikacijski.

Fizički sloj osigurava prijenos jedinica informacija i bavi se sklopovljem i električnim osobitostima signala, a sastoji se od medija, mehaničkih svojstava, konektora, električkih svojstava i procedure uspostava i prekida veze [1]. Ovdje spadaju RS-232, RJ45, V.35, V.34, I.430, I.431, T1, E1 te mnogi drugi.

Podatkovni sloj ostvaruje siguran prijenos podataka između dviju ili više točaka, formira pakete i podatkovne okvire dodavanjem i uklanjanjem zaglavlja, provjerava ispravnost podataka te upravlja protokom podataka. U ovaj se sloj ubrajaju 802.3, 802.11 a/b/g/n, MAC/LLC, ATM, HDP, FDDI, ARP, RARP, DCAP i ostali.

[1] Open systems interconnection

Mrežni sloj prenosi pakete podataka unutar i između mreža, upravlja zagušenjima, uspostavlja prividni put između računala i čvorova mreže, evidentira promet te transformira adrese. U ovaj sloj spadaju IP, ICMP, IGMP, IPsec, IPX te AppleTalk.

Prijenosni sloj rastavlja informacije na pakete, osigurava ispravan redoslijed paketa u prijemu, rastavlja razgovor u više veza i obrnuto, omogućava paralelne procese na računalu te upravlja prijenosom s kraja na kraj [1]. U ovom sloju se odvija komunikacija među računalima po izvršenim zadaćama prethodne razine. Omogućava očuvanje integriteta podataka između pošiljatelja i odredišta koristeći mehanizam ustanovljavanja greške i ponavljanja prijenosa do ispravnosti. Ovom sloju pripadaju TCP, UDP, SCTP, DCCP te SPX.

Sesijski sloj se bavi uspostavom veze između krajnjih korisnika i njenom sinkronizacijom, omogućava komunikaciju kroz mrežu te razdiobu nadzora korisnika nad zadaćom, a najlakše ga je objasniti kod videa putem Interneta kad ne želimo imati sliku bez tona ili obrnuto. Primjeri za ovaj sloj su SAP, L2TP, PPTP te SPDY.

Prezentacijski sloj postoji zbog kodiranja računalnih podataka na razne načine. Također se omogućava ispravna i razumljiva veza između učesnika i mreže i učesnika samih. Podaci se kodiraju na način da se korisniku mogu prikazati na njegovoj radnoj postaji. Njemu pripadaju TDI, ASCII, EBCDIC, MIDI, MPEG.

Aplikacijski sloj obavlja korisničke poslove kao što su e-pošta, prijenos datoteka, udaljeni terminalski rad i slično te predstavlja protokole i funkcije koje omogućavaju ispravno komuniciranje korisničkih aplikacija s podacima. Ovom sloju pripadaju NNTP, SIP, SSI, DNS, FTP, HTTP, NFS, NTP, SMPP, SMTP, SNMP i ostali.

TCP/IP[2] je skup protokola prihvaćen kao standard zbog pogodnosti koje je jedini u danom trenutku nudio, a to su neovisnost o tipu računalne opreme i operacijskih sustava, neovisnost o tipu mrežne opreme na fizičkoj razini i prijenosnog medija, jedinstveni način adresiranja koji omogućava povezivanje i komunikaciju svih uređaja koji podržavaju TCP/IP te standardizirani protokoli viših razina komunikacijskog modela, što omogućava široku primjenu mrežnih usluga [1]. Dva najčešće korištena protokola su TCP i IP, odakle i naziv. TCP je viši sloj i on upravlja sastavljanjem poruka ili datoteka u manje pakete koji se prenose preko Interneta. Donji sloj, IP, obrađuje adresni dio svakog paketa kako bi stigao na točno

[2] Transmission control protocol/Internet protocol

odredište. Svaki korisnik računala provjerava tu adresu kako bi znao gdje proslijediti poruku. TCP/IP koristi klijent/server model komunikacije u kojem korisnik računala zahtijeva i pruža uslugu od strane drugog računala u mreži [1]. TCP/IP protokol danas je prisutan na skoro svim računalima zbog jednostavnog definiranja adresa uređaja te zbog mogućnosti povezivanja na Internet. Svaki sloj ima svoju strukturu i terminologiju koja opisuje tu strukturu. Na aplikacijskom sloju TCP protokol za podatke koristi naziv tok, dok se kod UDP protokola koristi naziv poruka. TCP/IP model ima četiri sloja, a to su aplikacijski, prijenosni, Internet sloj i sloj mrežnog pristupa. Ova četiri sloja obuhvaćaju sve funkcionalnosti OSI modela. Aplikacijski sloj uključuje slične funkcije gornja tri OSI sloja, a sloj mrežnog pristupa uključuje slične funkcije donja dva OSI sloja. Oba modela koriste slojeve za prikaz komunikacije te imaju slične uloge. TCP/IP se može koristiti kao komunikacijski protokol u privatnoj mreži. Protokoli unutar TCP/IP modela su PPP, PPTP, CSMA/CD, HTTP, FTP, Telnet, POP, SMTP, SNMP, DNS, DHCP.

OSI model je standardni referentni model koji opisuje kako različite softverske i hardverske komponente uključene u mrežnu komunikaciju trebaju podijeliti rad i interakciju jedan s drugim, dok TCP/IP model opisuje dva mrežna standarda koji definiraju Internet [6]. IP definira kako računala mogu međusobno dobiti podatke preko usmjerenog skupa mreža, a TCP definira kako aplikacije mogu stvoriti pouzdane komunikacijske kanale preko takve mreže. Uglavnom, IP definira adresiranje i usmjeravanje, a TCP definira kako se odvija razgovor preko linka bez gubitka podataka.

3. Klasifikacija protokola u funkciji računalnih mreža

Mrežni protokoli se mogu klasificirati prema slojevima kojima pripadaju bilo da je riječ o OSI modelu ili TCP/IP modelu. U prethodnom poglavlju navedeni su svi važniji protokoli za sve slojeve oba modela, a u ovom će poglavlju svaki protokol biti detaljno opisan. Nisu svi navedeni pripadajući elementi nužno i mrežni protokoli, već su neki od njih i fizički elementi odnosno pomagala pri procesu prijenosa informacija.

Krene li se od fizičkog sloja, može se reći da se on sastoji od medija, konektora i mehaničkih svojstava. Fizički sloj osigurava prijenos jedinica informacija i bavi se sklopovljem i električnim osobitostima signala. RS-232 je standardni međusklop koji pomaže pri serijskom prijenosu binarnih podataka između datotečne spojne opreme DTE[3] i datotečne komunikacijske opreme DCE[4] [18]. RS-232 se koristi i kao standardni serijski međusklop na računalima, ali ga noviji serijski međusklopovi poput USB-a[5] istiskuju iz upotrebe.

RJ45 je standardizirano telekomunikacijsko mrežno sučelje ili konektor za povezivanje glasa i opreme podataka na pružene usluge od strane lokalne razmjene nosioca ili nosioca na veće udaljenosti. Specifikacija uključuje fizičku izgradnju, ožičenje i signalnu semantiku. RJ konektora ima nekoliko vrsta, a RJ45 se koristi pretežito kod *Etherneta*[6] u računalnim mrežnim specifikacijama. V.35 je specifikacija koja omogućava odabir tipa konektora, dodjelu PIN-a i odabir razine signala, a koristi se u sinkronim komunikacijskim sučeljima. V.34 je standard za *full duplex* modeme koji šalju i primaju podatke preko telefonske linije brzinama do 33.8 kbit/s automatskim podešavanjem brzine transmisije temeljene na kvaliteti linije.

Na podatkovnom sloju se javljaju bitni protokoli za ostvarenje sigurnog prijenosa podataka. Podatkovni sloj formira pakete i podatkovne okvire dodavanjem i uklanjanjem zaglavlja, provjerava ispravnost podataka, upravlja protokom podataka [1]. IEEE 802.3 je radna skupina standarda i LAN[7] tehnologija s nekim WAN[8] aplikacijama. Fizička veza je

[3] Data terminal equipment
[4] Data circuit-terminating equipment
[5] Universal serial bus
[6] IEEE 802.3 – Mrežna tehnologija za LAN mreže
[7] Local area network

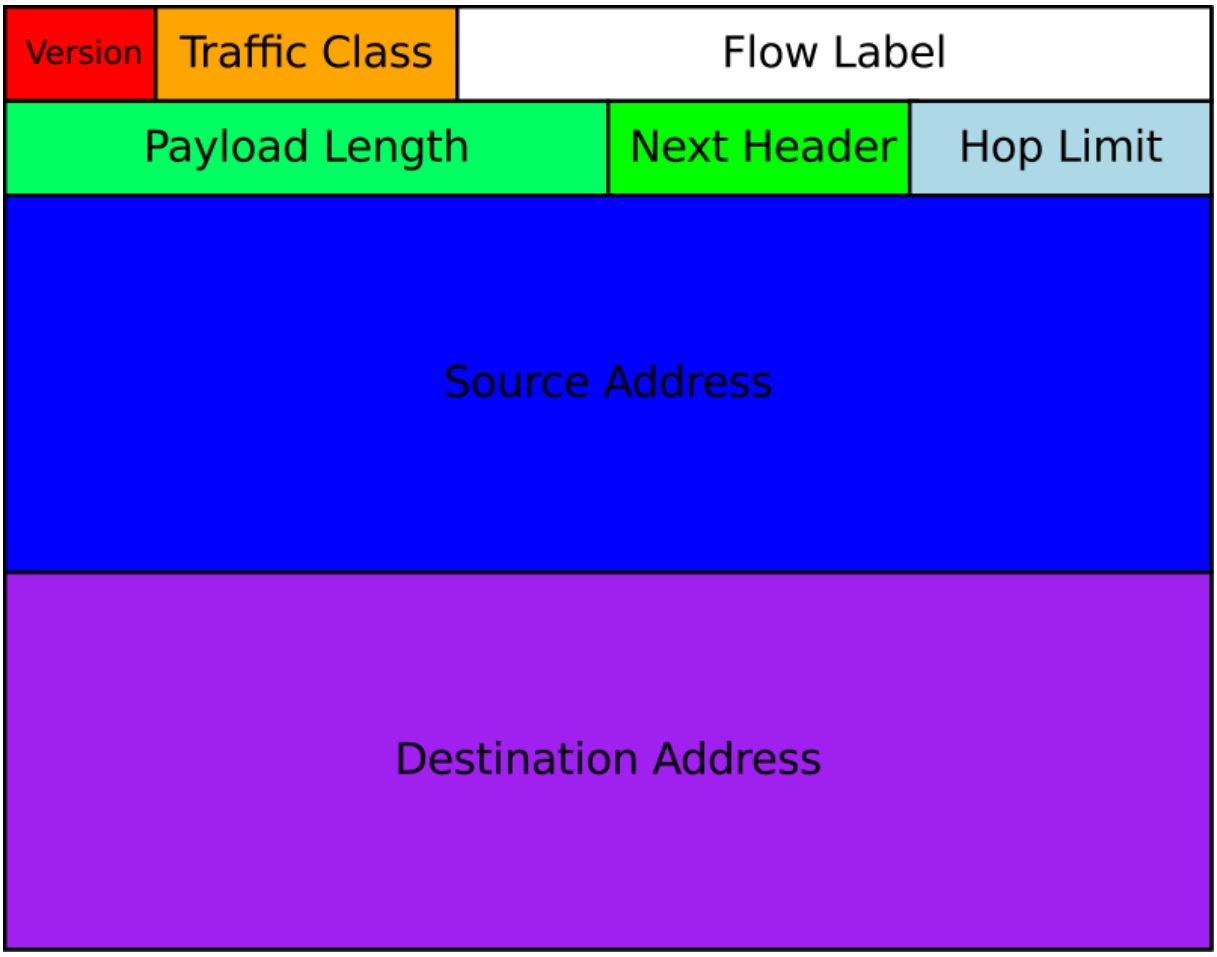
između čvorova i infrastrukturnih uređaja poput koncentratora, preklopnika i usmjerivača pomoću različitih tipova bakra i kablova od vlakana. Ova tehnologija podržava mrežnu arhitekturu IEEE[9] 802.1 te definira LAN metodu pristupa pomoću CSMA/CD. CSMA/CD je višestruki pristup s detekcijom sudara, odnosno, metoda kontrole pristupa mediju koja se prvotno koristi u LAN tehnologiji koristeći *Ethernet* tehnologiju. Koristi se za poboljšanje performansi tako što raskida transmisiju čim sudar biva otkriven te za skraćenje vremena potrebnog za ponovni pokušaj. IEEE 802.11 je bežična mreža gdje se podaci između dvaju ili više računala prenose pomoću radio frekvencija i odgovarajućih antena. Koristi se za WLAN mreže. Trenutno sadrži šest načina bežične modulacije signala. Postoje četiri standarda, a, b, g i n. A standard koristi frekvencije na 5 GHz, dok ostali standardi koriste frekvencije na 2.4 GHz. Proizvodi napravljeni prema ovim standardima nose zaštitni znak *Wi-Fi*. MAC u podatkovnom sloju predstavlja podsloj, a označava kontrolu pristupa mediju. MAC podsloj omogućava adresiranje i kontrolu pristupa kanalu. MAC podsloj djeluje kao sučelje između kontrole logičke poveznice (LLC) i fizičkog sloja. LLC predstavlja gornji podsloj podatkovnog sloja [1]. LLC pruža multipleksiranje mehanizama za mrežne protokole IP, IPX i AppleTalk. LLC djeluje kao sučelje između kontrole pristupa mediju (MAC) i mrežnog sloja.

ATM predstavlja spojnu tehniku komuniciranja što znači da se prije svakog prijenosa korisničkih informacija između izvora i odredišta mora uspostaviti veza, a prilikom završetka tog prijenosa veza se raskida. ATM također može podržati i prijenos nespojnih usluga, odnosno datagram uslugu. Osnovna usluga koju ovaj protokol pruža višim protokolnim slojevima je komutacija ćelija. U ATM mrežama postoje 3 vrste veza, a to su trajne, polutrajne i veze koje se uspostavljaju na zahtjev. Trajne veze se koriste za signalizaciju i mrežno upravljanje, ali se ne uspostavljaju signalizacijskim procedurama. Polutrajne veze uspostavlja mrežni operater na zahtjev korisnika i za ove se veze koristi još i naziv trajna virtualna veza (PVC). Takve veze nakon isteka određenog vremena raskida sama mreža ili ih ručno raskida operater. Veze na zahtjev uspostavljaju se pomoću signalizacijskih protokola na inicijativu pozivajućeg korisnika. Za ove se veze još koristi naziv komutirana virtualna veza (SVC) čija se uspostava temelji na signalizaciji u stvarnom vremenu. FDDI protokol omogućava prijenos digitalnih podataka od 100 Mbit/s i optički je standard prijenosa podataka na LAN mreži koja se može protezati i do 200 km. Obično su osnova WAN mreža i

[8] Wide area network
[9] Institute of electrical and electronics engineers

razvijen je kao potreba za brži i pouzdaniji prijenos podataka preko računalnih mreža. ARP je komunikacijski protokol kojim se na lokalnoj mreži iz poznate mrežne adrese dobiva fizička adresa, odnosno IP adresu prevodi u MAC adresu. Najraširenija primjena je na *Ethernetu* gdje se IP adrese povezuju s MAC adresama dok RARP protokol ima funkciju obrnutu ARP-u, a to je da iz poznate MAC adrese saznaje IP adresu.

Mrežni sloj kontrolira rad podmreže i odlučuje kojim fizičkim putem podaci trebaju biti poslani ovisno o mrežnim uvjetima i prioritetu usluga. On omogućava usmjeravanje, kontrolu prometa, fragmentaciju okvira te prevođenje logičkih adresa u fizičke. Upravlja zagušenjima, uspostavlja prividni put između računala i čvorova mreže, evidentira promet te transformira adrese [1]. IP protokol je protokol za komunikaciju između izvora i korisnika putem Interneta. Na ovom se protokolu podaci između modema šalju u paketima, a protokol je nepouzdan jer ne osigurava prijenos podataka u ispravnom stanju i ne osigurava da će podaci uopće i doći do odredišta. Predajnik i prijamnik se ne dogovaraju o početku i završetku prijenosa podataka, nego predajnik pošalje paket, a prijamnik ne šalje potvrdu o primitku istoga. Svaki uređaj na mreži se identificira pomoću IP adrese. Postoje dvije verzije IP protokola, a to su IPv4 i IPv6. IPv4 koristi 32-bitnu IP adresu, odnosno dužina svake IP adrese u ovoj verziji iznosi 32 bita. S obzirom na tu dužinu, maksimalni broj adresa iznosi 4.3 milijardi. Zbog sve većeg broja računala, aparata, mobilnih uređaja pa čak i kućanskih uređaja ovaj broj je postao nedovoljan pa je razvijena verzija IPv6. IPv6 je standardna verzija komunikacijskog protokola na Internetu, a koristi 128-bitnu IP adresu. Širenje interneta i rast potrebe za novim IP adresama doveli su do razvoja ove verzije protokola. Osim većeg adresnog prostora ovaj protokol nudi i prednosti poput prijenosa paketa prema više odredišta u jednom procesu slanja, sigurnost mrežnog sloja te pojednostavljeno prosljeđivanje paketa.



Slika 1. IPv6, zaglavlje paketa [19]

ICMP protokol operacijski sustavi koriste za rješavanje grešaka na mreži, najčešće kada određena usluga nije dostupna. Ugrađen je u svaki IP modul da bi omogućio mrežnim ruterima ili računalima slanje kontrolnih poruka o greškama. Zadatak mu je da samo prijavi pogrešku, ali ne i da ju ispravlja. Osnovna namjena je osigurati nadzor i kontrolu prijenosa podataka do odredišta, s obzirom da to IP protokol ne osigurava. Šalje poruke koje osiguravaju kontrolu toka, prijavu pogreške, pojavu alternativnog puta do odredišta i druge informacije namijenjene samoj programskoj podršci [3]. IPsec je skup protokola za sigurnu komunikaciju IP-a autentikacijom i enkripcijom svakog IP paketa komunikacijske sesije. Ovaj skup protokola uključuje protokole za uspostavljanje zajedničkih autentikacija između agenata na početku sesije i pregovaranja kriptografskih ključeva koji će se koristiti za vrijeme sesije. Mogu se koristiti u zaštiti podataka tokova, između para sigurnosnih poveznika ili

između sigurnosnih poveznika i *hostova*[10]. IPsec koristi kriptografske sigurnosne usluge za zaštitu komunikacija putem IP mreža i podržava integritet podataka, tajnost podataka i zaštitu ponavljanja.

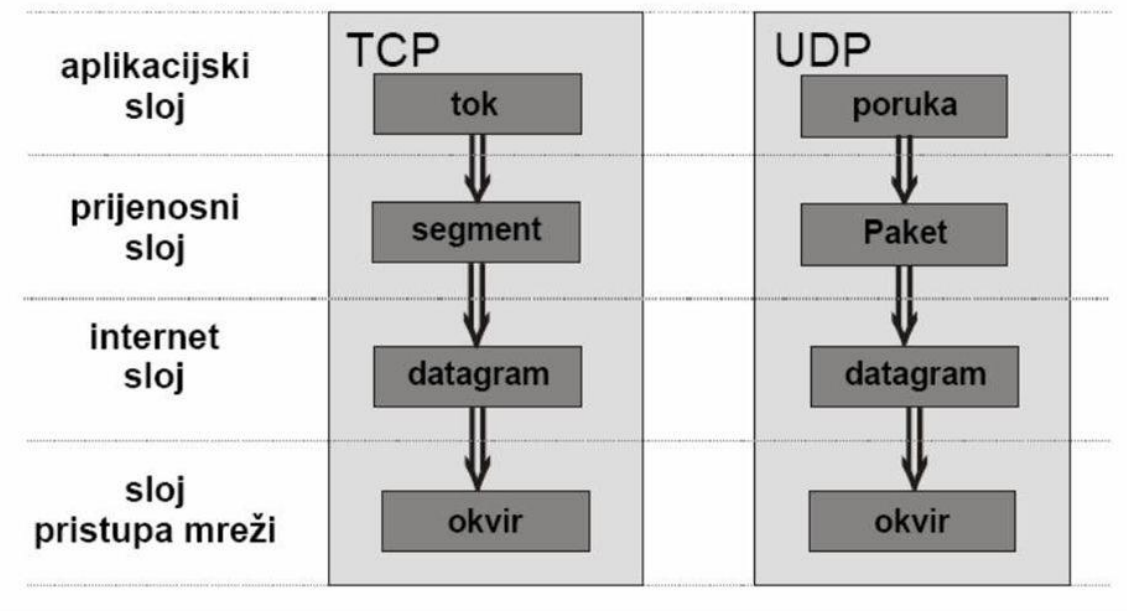
Prijenosni sloj zadužen je za pouzdan prijenos podataka između uređaja. Otkriva i ispravlja greške u prijenosu i osigurava da se poruke isporučuju bez pogreške, gubitaka ili dupliciranja. Prijenosni sloj pruža segmentaciju poruka, kontrolu protoka poruka i multipleksiranje sesija. Rastavlja informacije na pakete, osigurava ispravan redoslijed paketa u prijemu, rastavlja razgovor u više veza i obrnuto, omogućava paralelne procese na računalu te upravlja prijenosom s kraja na kraj [1]. TCP protokol osigurava pouzdanu uslugu prijenosa s uspostavljanjem konekcije od izvorišta do odredišta. Podatkovne jedinice nazivaju se segmenti koji se pakiraju u IP pakete i šalju preko mreže. Osnovna svojstva koja pruža su pouzdanost, veza od točke do točke te dvosmjerni prijenos podataka. Prilikom korištenja TCP protokola entiteti prolaze kroz tri faze a to su uspostava veze, razmjena podataka i prekid veze. TCP je pouzdan jer za svaki poslani segment očekuje potvrdu prijema. Ako nakon isteka određenog vremenskog perioda ne dođe pozitivna potvrda, ili dođe informacija o netočno primljenim podacima, prijenos se ponavlja sve dok ne dođe pozitivna potvrda o prijemu. UDP protokol je uz TCP jedan od temeljnih protokola. Ne osigurava pouzdan prijenos podataka i ne uspostavlja vezu. Omogućava slanje kratkih poruka između aplikacija na umreženim računalima. Nema mogućnost provjere primitka poruke jer ne čuva informaciju o stanju veze. Koristi se kada su efikasnost i brzina bitniji od pouzdanosti za što je najbolji primjer prijenos govora u realnom vremenu te kada je potrebno slanje iste poruke na više odredišta. Koristi IP protokol, a omogućava protokolima više razine slanje poruka drugim programima uz minimalno korištenje mehanizama protokola. SCTP protokol služi za transmisiju više strujanja podataka istovremeno između dvije krajnje točke koje su uspostavile vezu na mreži. SCTP osigurava pouzdan prijenos podataka kao i TCP, ali i osigurava potpuni dolazak podatkovnih jedinica koje se šalju preko mreže. Uz to, osigurava i potpuni istodoban prijenos više tokova podataka između povezanih krajnjih točaka.

[10] Bilo koji uređaj povezan u računalnu mrežu

UDP datagram	
16-bit source port number	16-bit destination port number
16-bit length	16-bit UDP checksum
Data	

Slika 2. UDP zaglavlje [10]

UDP zaglavlje sastoji se od četiri polja, svako po dva bajta, što ukupno daje 16 bitova. Upotreba polja *Checksum*[11] i *Source port*[12] nije obavezna u protokolu IPv4. U IPv6 protokolu samo *Source port* nije obavezan. Druga dva polja su broj ciljnog porta te dužina.

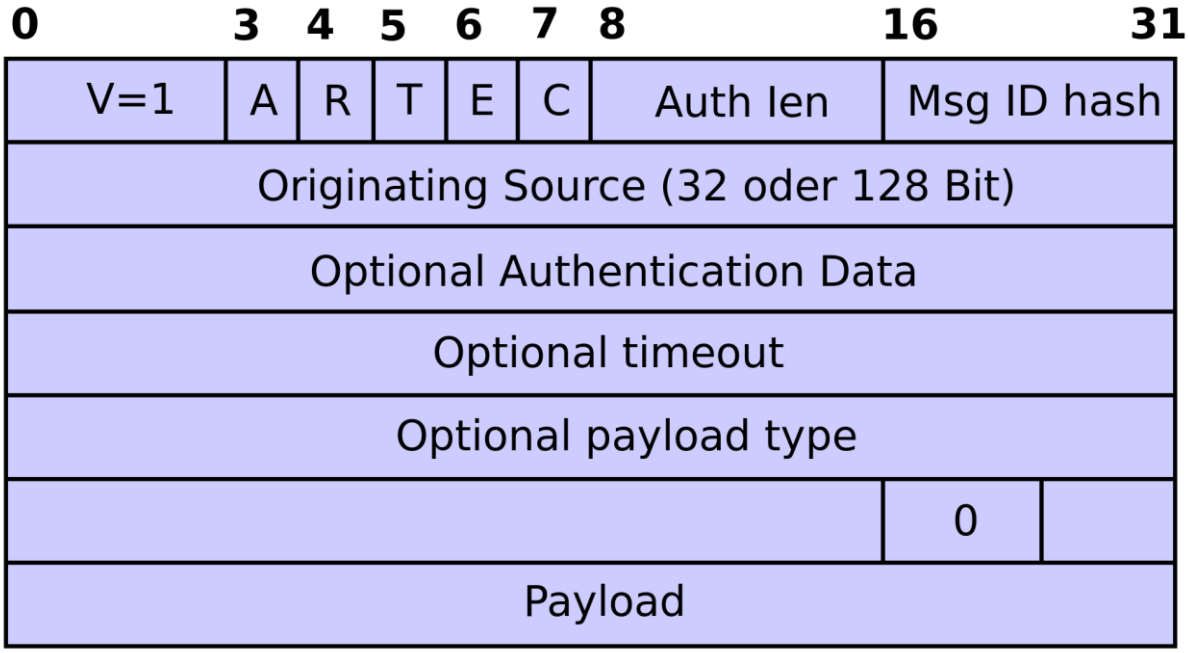


Slika 3. Struktura podataka po slojevima TCP/IP modela [10]

Sesijski sloj omogućava osnivanje sesija između procesa pokrenutih na različitim stanicama te omogućava uspostavu sesija, održavanje sesija, omogućava uspostavu dva aplikacijska procesa na različitim stanicama. Podrška sesije obavlja funkcije koje

[11] Kontrolna suma, koristi se za provjeru grešaka u zaglavlju i podacima
[12] Polazni port, identificira port pošiljatelja

omogućavaju tim procesima komunikaciju putem mreže, sigurnost i prepoznavanje imena. Sloj sesije također uspostavlja, upravlja i prekida veze između aplikacija. Sesijski sloj se bavi uspostavom veze između krajnjih korisnika i njenom sinkronizacijom, omogućava komunikaciju kroz mrežu te razdiobu nadzora korisnika nad zadaćom. SAP je protokol koji služi za objavu sjednice svim zainteresiranim sudionicima korištenjem višeodredišnog razašiljanja preko poznate adrese. Ovaj protokol spada u grupu protokola za podršku sesije, a druga dva su SDP i SIP. SDP je protokol za opis sjednice, a sadrži podatke o protokolima i formatima koji će se koristiti u sesiji, dok SIP protokol služi za pokretanje sesije, razmjenu podataka o sesiji te za poziv za sudjelovanje u sesiji određenom korisniku. SAP periodički razašilje objavu ili administrativno određenu višeodredišnu adresu. Zainteresirani sudionici osluškuju objave i po želji se priključuju sesiji. Kod SAP protokola se javlja i jedan potencijalni problem, a to je prilagodba veličini gdje problem nije u broju sudionika, već u broju objava sesija. SAP je pogodan za javne sesije kod kojih se sudionici ne znaju unaprijed.



Slika 4. SAP paket [10]

L2TP je protokol tuneliranja koji se koristi za podršku virtualne privatne mreže ili kao dio pružanja usluga od strane davatelja internetskih usluga. Po sebi, to ne pruža nikakvu

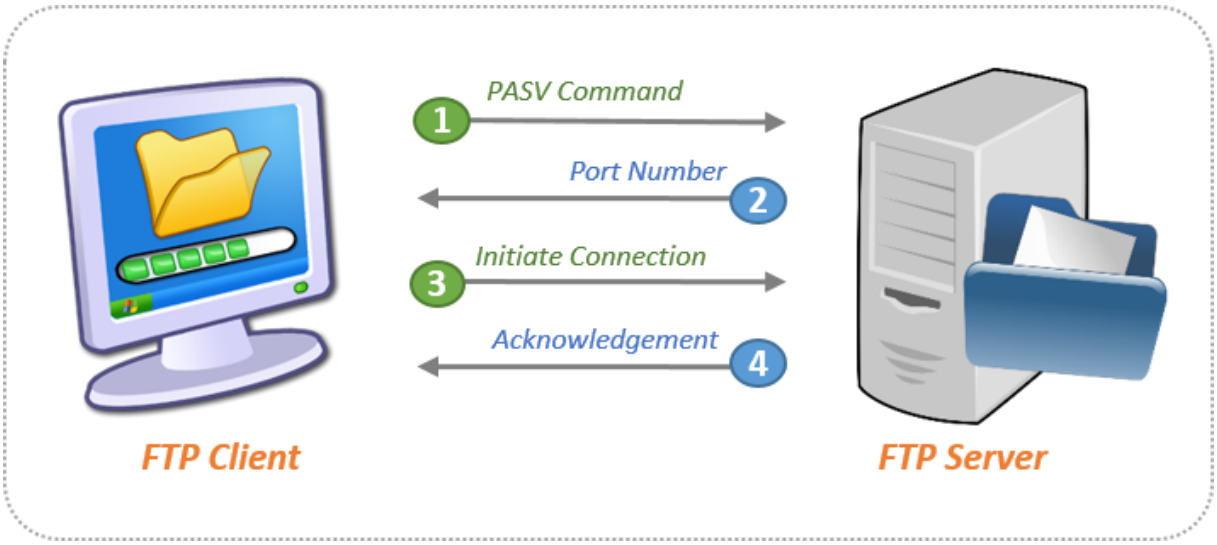
enkripciju ili povjerljivost. Umjesto toga, povjerljivost se oslanja na protokol šifriranja koji prolazi tunelom radi provedbe privatnosti. PPTP protokol je metoda za provedbu virtualne privatne mreže koji koristi kontrolni kanal preko TCP tunela. PPTP specifikacija ne opisuje šifriranje ni mogućnosti provjere autentičnosti. PPTP je bio predmet mnogih sigurnosnih analiza i pronađeni su mnogi sigurnosni propusti u njemu. SPDY je otvoreni mrežni protokol razvijen prvenstveno na *Googleu* za transport web sadržaja. On manipulira HTTP promet s ciljevima smanjenja latencije učitavanja web stranica i poboljšanja sigurnosti na mreži. Ono što postiže je smanjena latencija putem kompresije, multipleksiranje i prioritizacija iako, to ovisi o kombinaciji razvoja uvjeta mreže i web stranica.

Prezentacijski sloj postoji zbog kodiranja računalnih podataka na razne načine. Također se omogućava ispravna i razumljiva veza između učesnika i mreže i učesnika samih. Podaci se kodiraju na način da se korisniku mogu prikazati na njegovoj radnoj postaji. Također omogućuje da podaci budu čitljivi na odredištu, brine o formatu i strukturi podataka i pregovara o sintaksi prijenosa za aplikacijski sloj. Formatira podatke koji će biti prezentirani na aplikacijskom sloju. Odgovoran je za konverziju podataka, konverziju skupa protokola, konverziju karaktera, kompresiju podataka i šifriranje podataka [1]. Podaci se na prezentacijskom sloju prevode u prepoznatljiv oblik. ASCII[13] je američki standardni znakovnik za razmjenu informacija, a predstavlja način kodiranja znakova temeljenih na engleskoj abecedi. ASCII kodovima predstavlja se tekst u računalima, komunikacijskoj opremi i drugim napravama koje obrađuju tekst pisan na engleskom jeziku. Većina modernih shema za kodiranje se temelji na ASCII kodu. ASCII kodira 128 navedenih znakova u sedam-bitne brojeve. Znakovi koji se kodiraju su brojevi od 0 do 9, mala slova od a do z, velika slova od A do Z, interpunkcijski simboli i kontrolni kodovi. MIDI predstavlja standardni međusklop koji omogućava spajanje elektronskih glazbala, računala i ostalih glazbenih uređaja i usklađuje razmjenu podataka između tih uređaja. MIDI ne razmjenjuje analogne signale, već digitalne koji opisuju zvuk koji je uređaj stvorio. MPEG predstavlja standard koji specificira postupke simultanog kodiranja sintetičkih i prirodnih objekata i zvukova. To je standard za audio-video kodiranje kako bi se zadovoljile različite potrebe komunikacijskih, interaktivnih i difuznih modela servisa. MPEG osigurava skup tehnologija da bi zadovoljio potrebe autora. Autorima MPEG osigurava produkciju sadržaja koji ima veću mogućnost da se ponovno koristi i veću

[13] American standard code for information interchange

fleksibilnost nego što je to moguće primjenom pojedinih tehnologija kao što su digitalna televizija, animirana slika i web stranice. MPEG omogućava prikazivanje audio, video i audio-video sadržaja, opisivanje kompozicije objekata, multipleksiranje i sinkronizaciju podataka te interakcije s audio-video scenama.

Aplikacijski sloj obavlja korisničke poslove kao što su e-pošta, prijenos datoteka, udaljeni terminalski rad i slično te predstavlja protokole i funkcije koje omogućavaju ispravno komuniciranje korisničkih aplikacija s podacima. Upućuje zahtjev za uslugama prezentacijskog sloja te pruža usluge aplikacijama, a ne krajnjem korisniku [1]. Bitne funkcije aplikacijskog sloja su dijeljenje resursa i preusmjeravanje uređaja, daljinski pristup datotekama, upravljanje mrežom, elektronička pošta. NNTP je protokol koji služi za prenošenje članaka između poslužitelja kao i za čitanje i slanje vijesti od strane krajnjih korisnika. SSI protokol je jednostavan komunikacijski protokol dizajniran za prijenos podataka između računala i korisničkih terminala i pametnih senzora. Koristi se u komunikacijama od točke do točke, a kriteriji za razvoj su opća namjena, jednostavnost korištenja i mali tragovi na strani poslužitelja. DNS je baza podataka u kojoj su upisana sva imena i odgovarajuće IP adrese pojedinih računala te grupa funkcija koje omogućavaju prevođenje istih. Komunikacija između pojedinih računala u nekoj mreži se zasniva na principu IP adresa koje su potpuno određene. Zbog razloga što je teško zapamtiti i zadržati preglednost nad velikim brojem adresa, uveden je sistem koji adresu jednog računala veže za jedno ime, a to sve je pohranjeno upravo u DNS-u. FTP je protokol koji se koristi za premještanje datoteka s jednog *hosta* na drugi putem mreže temeljene na TCP-u. Sagrađen je na korisničko-serverskoj arhitekturi i koristi odvojeno nadzornu i podatkovnu vezu između korisničkog računala i servera. FTP veza se uspostavlja na zahtjev korisničkog računala prema serverskom računalu. Korisničko računalo mora posjedovati program koji implementira FTP protokol, a serversko računalo mora posjedovati program koji prihvaća veze na standardnom FTP portu te razumije komande FTP protokola.



Slika 5. Podešavanje FTP servera na OS Windows [20]

HTTP je glavna i najčešća metoda prijenosa informacija na Internetu. Osnovna namjena je omogućavanje objavljivanja i prezentacije HTML dokumenata, odnosno web stranica. HTTP je protokol za komunikaciju između poslužitelja i klijenta [3]. HTTP klijent najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web serverom na određenom portu. HTTP se razlikuje od ostalih protokola po tome što se konekcija i komunikacija sa serverom prekidaju odmah nakon izvršenja zahtjeva klijenta. Upravo zbog toga je HTTP idealan za web, gdje je stranica najčešće povezana s drugim stranicama na drugim poslužiteljima. SMPP je otvoreni standardni protokol dizajniran za osiguravanje fleksibilnosti sučelja za prijenos podataka za prijenos kratkih poruka između vanjskih entiteta, entiteta usmjeravanja i centara poruka. SMPP se često koristi kako bi se omogućilo treće stanje da podnese poruke koje su često u rasutom stanju. SMTP je uobičajeni način za prijenos elektroničke pošte na Internetu. Brine o slanju e-pošte na neko drugo računalo. E-pošta se prvo šalje na SMTP server, a potom do drugog servera i do odredišta. SMTP može prenositi samo tekst, a ne može binarne podatke, kao ni slike, zvuk ili filmove. Koristi MIME protokol koji mu omogućava slanje binarnih podataka preko TCP/IP mreže, a MIME protokol binarne podatke preoblikuje u tekst i predstavlja proširenje standarda za elektroničku poštu koja omogućava prijenos i drugih podataka osim standardnih 7-bitnih znakova. Osigurava pouzdan i efikasan prijenos elektroničke pošte između pošiljatelja i primatelja. Posebna

prednost SMTP protokola je mogućnost prijenosa elektroničke pošte neovisno o prijenosnim sustavima na putu do odredišta. Zahtijeva jedino pouzdanu vezu za prijenos podataka.

4. Logička provjera mrežnih protokola

Svaki od navedenih protokola u prethodnom poglavlju ima svoju funkciju i zadaću. Jednom sloju, bilo da je riječ o OSI referentnom modelu ili o TCP/IP referentnom modelu, pripada više protokola koji zajedno omogućavaju slojevima obavljanje njihovih zadataka, a svaki od tih protokola se razlikuje međusobno po pojedinim detaljima. Korištenje pojedinog protokola moguće je utvrditi logičkom provjerom mrežnih protokola.

Logička provjera mrežnih protokola prikazuje i opisuje koji su se protokoli koristili na mreži za vrijeme obavljanja određenih funkcija. Analiza i provjera mrežnih protokola detaljno je prikazana i opisana u idućem poglavlju, a moguće ih je obavljati pomoću raznih alata od kojih se svaki sam po sebi razlikuje od ostalih.

Protokole je potrebno i istražiti s ciljem pronalaženja načina na koje je moguće formalno izgraditi povjerljive i učinkovite implementacije mrežnih protokola za industrijske sustave korištenjem modernih principa programiranja [22]. Krajnji cilj istraživanja je razviti neki okvir programiranja koji bi softverskim inženjerima dozvolio razvoj bilo koje vrste povjerljivih komunikacijskih skupina protokola. Jedan od ciljeva istraživanja protokola je i zadržavanje važnosti konteksta modernih razvojnih softvera. Svaka specifikacija mrežnih protokola obuhvaća dva glavna područja, a to su procesiranje poruka protokola što uključuje validaciju, enkripciju i kompresiju te semantika više razine definiranja protokola koja može biti prikazana kao vrsta reaktivnog sustava ili automat s konačnim brojem stanja koji može reagirati na poruke na ispravan način i koji se ne može staviti u nedefinirano stanje [22].

Logika za dokazivanje sigurnosnih svojstava mrežnih protokola koji koriste javne i simetrične kriptografske ključeve naziva se „protokolska kompozicijska logika“ [23]. Logika je dizajnirana na temelju procesa izračuna za moguće korake protokola kao što su stvaranje novih slučajnih brojeva te slanje i primanje poruka, a obavlja dešifriranje te akcije verifikacije digitalnog potpisa. Dva rezultata logike su skupina kompozicijskih teorema i računalna ispravnost teorema. Kompozicijski teoremi dozvoljavaju da dokazi kompleksnih protokola budu izgrađeni od dokaza njihovih sastavnih pod-protokola. Računalna ispravnost teorema jamči da dokazi u protokolskoj kompozicijskoj logici imaju isto značenje kao i kriptografski

dokazi. Ova metoda se uspješno primjenjuje na brojnim protokolima internetskih, bežičnih i mobilnih mreža.

Logička provjera protokola ne služi samo za prikaz korištenih protokola na mreži već pruža i dodatne mogućnosti koje pomažu korisnicima za lakše korištenje i razumijevanje istih. Na svakom od alata moguće je naučiti nešto novo o svakom protokolu jer detaljnim prikazom strukture korištenih protokola uočavaju se detalji i informacije za njih koji su ranije možda bili nejasni ili teže razumljivi.

Na ovaj način moguće je uočiti i pogreške koje su se događale prilikom prikupljanja i obrade paketa i podataka, a koje se također mogu ispraviti. Prikupljanjem i zbrajanjem podataka u jednu cjelinu vidljiva je detaljna struktura protokola s pripadajućim informacijama, ali i njihove nepravilnosti čijim se ispravljanjem omogućava brža analiza protokola u budućnosti i olakšava se rad korisnicima.

Postoji šest vrsta protokolskih pogrešaka, a to su redom:

- *unspecified reception*,
- *nonexecutable interaction*,
- *deadlock*,
- *livelock*,
- *state ambiguity* te
- *overflow*.

Unspecified reception je pogreška neutvrđenog prijema koja predstavlja prijem koji je izvršen, ali nije specificiran u dizajnu. S obzirom na to da potrebni prijem nije specificiran u dizajnu njegova pojava znači da sljedeće ponašanje sustava nije predvidljivo. *Nonexecutable interaction* predstavlja transmisiju ili prijem koji je specificiran u dizajnu, ali nikad ne biva izvršen. Često se zbog toga naziva „mrtvim kodom“. *Deadlock* stanje se javlja kad svi procesi mogu ostati neodređeni jedino u istom stanju. To znači da je *deadlock* globalno stanje dostupno s početnog globalnog stanja u kojem su svi kanali prazni s nemogućnošću transmisije. *Deadlock* se mora izbjegavati zbog toga što sustav biva blokiran zauvijek ako jednom dođe u *deadlock* stanje. *Livelock* je situacija u kojoj nekoliko procesa razmjenjuje poruke, ali bez ikakvog efektivnog rada koji bi bio izvršen prema obavljanju svojih servisa. Ponekad se naziva i „*dynamic deadlock*“ i također se mora izbjegavati jer ako se jednom

pojavi ostaje zaključan unutar male grupe globalnih stanja. *State ambiguity* odnosno stanje neodređenosti postoji kada stanje u jednom procesu može koegzistirati stabilno, što znači da je dostupno s praznim kanalima, s više od jednog stanja u nekom drugom procesu. Procesi unutar komunikacijske mreže se često izvršavaju u visoko sinkronim manirima. Prema tome se da zaključiti da ovo stanje nužno ne predstavlja pogrešku, već treba biti pažljivije razmatrano. *Overflow* je stanje kanala u kojem broj poruka unutar kanala nije ograničen predefiniranim pozitivnim cijelim brojem. To znači da svaki komunikacijski kanal ima kapacitet pohrane koji ograničava iznos informacija koje može prenositi u određenom trenutku. U pokušaju povećanja tog kapaciteta može doći do gubitka podataka koji se prenose među procesima. *Overflow* se javlja u dva različita stanja, *finite overflow* te *infinite overflow*. *Finite overflow* ukazuje na to da su kanali ograničeni jednim brojem, ali ne predefiniranim, dok *infinite overflow* ukazuje da kanali nikad nisu ograničeni. *Finite overflow* može biti dinamički riješen, dok *infinite overflow* ukazuje na mogućnost postojanja potencijalnih pogrešaka. Protokol je dobro formiran ako ne sadrži nespecificirane prijeme i ako nema *nonexecutable interaction* pogreške. Protokol je „živ“ ako je slobodan od *deadlock* situacija i nespecificiranih prijema. U toj situaciji protokol će uvijek napredovati, a siguran je ako je „živ“ i uvijek se ispravno izvršava [25].

Ono što je bitno napomenuti jest i kontrola zagušenja. Zagušenje nastaje u situacijama kada mrežni čvor prenosi više podataka nego što ih može obraditi. Posljedice toga su kašnjenje paketa, gubitak paketa i blokiranje novih konekcija. Vrlo je bitno da se zagušenje izbjegne, a postoje dvije metode za kontrolu zagušenja. Jedna od njih je *end-to-end* gdje mrežni sloj ne pruža eksplicitnu podršku transportnom sloju za svrhu kontrole zagušenja. Mora se zaključiti i sama prisutnost zagušenja krajnjim sustavima baziranim samo na promatranom ponašanju mreže kao što su kašnjenje i gubitak paketa. Druga metoda je kontrola zagušenja uz pomoć mreže. Kod ove metode komponente mrežnog sloja, odnosno modemi, pružaju eksplicitnu povratnu informaciju pošiljatelju u pogledu stanja zagušenja na mreži. Ta povratna informacija može biti jednostavna kao jedan bit koji ukazuje na zagušenje na vezi. Jedan od primjera ove kontrole jest ATM ABR kontrola. ABR protokol je protokol koji koristi mrežni pristup prema kontroli zagušenja. Ovdje je cilj ilustrirati protokol koji se značajno razlikuje po pristupu prema kontroli zagušenja od ostalih protokola. ATM koristi virtualno-kružni orijentirani pristup prema prebacivanju paketa. ABR je dizajniran kao

elastična usluga prijenosa podataka na način koji podsjeća na TCP. Kad je mreža preopterećena, ABR usluga bi trebala biti u mogućnosti iskoristiti prednost rezervne dostupne širine, a kada je mreža zagušena, ABR bi trebao smanjiti razinu prijenosa na neku unaprijed određenu minimalnu razinu prijenosa.

Jedan od jednostavnijih načina otkrivanja pogrešaka jest upotreba jedinstvenog pariteta. Uređaj koji koristi ovaj način je prijamnik. Ako se u parnoj shemi pariteta pojavi neparan broj bitova, prijamnik zna da se dogodila barem jedna pogreška. Ako se pojavi paran broj pogrešaka to bi rezultiralo nezapaženom pogreškom. Ako je vjerojatnost pogrešaka mala i pretpostavi se da će se pogreške pojavljivati neovisno jedna o drugoj, vjerojatnost višestrukih pogrešaka unutar paketa bila bi vrlo mala. Prijamnik ima mogućnost uočavanja i ispravljanja pogrešaka koja se naziva FEC[14] (*forward error correction*). Ove tehnike su vrijedne jer mogu smanjiti broj potrebnih ponovnih prijenosa od strane pošiljatelja te dozvoljavaju korekciju pogrešaka čim se primijete.

Tehnika detekcije pogrešaka koja je danas također rasprostranjena u računalnim mrežama bazirana je na CRC[15] (*cyclic redundancy check*) kodovima. Ciklička provjera redundancije je kod za otkrivanje pogrešaka koji se obično koristi u digitalnim mrežama i uređajima za pohranu radi otkrivanja slučajnih promjena neobrađenih podataka. Blokovi podataka koji ulaze u takve sustave dobivaju kratku kontrolnu vrijednost prilagođenu na temelju ostatka dijela polinoma njihovog sadržaja. Izračun se ponavlja prilikom preuzimanja i, u slučaju da se vrijednosti ne podudaraju, mogu se poduzeti korektivne mjere protiv korupcije podataka. CRC kodovi se tako nazivaju jer je vrijednost provjere podataka redundancija, a algoritam je baziran na cikličkim kodovima. Jednostavni su za implementaciju u binarnom hardveru te za analizirati ih matematički i dobri za uočavanje uobičajenih pogrešaka uzrokovanih bukom u prijenosnim kanalima.

Valja napomenuti i TCP kontrolu zagušenja. TCP je protokol koji pruža pouzdanu uslugu prijenosa između dva procesa koji se odvijaju na različitim računalima. Druga važna značajka ovog protokola jest mehanizam nadzora nad zagušenjima. TCP mora koristiti kontrolu zagušenja od kraja do kraja jer IP sloj ne daje povratnu informaciju krajnjim sustavima koji se odnose na zagušenje mreže. Kod TCP pristupa svaki pošiljatelj mora

[14] Tehnika za kontroliranje pogrešaka u prijenosu datoteka
[15] Kod korišten u digitalnim mrežama

ograničiti stopu na kojoj šalje promet u svoju vezu kao funkciju zapaženog mrežnog zagušenja. Ako pošiljatelj uoči da je i najmanja količina zagušenja na putu od njega do odredišta, mora povećati stopu slanja. Iz toga proizlaze tri bitna pitanja, kako pošiljatelj ograničava stopu na kojoj šalje promet u konekciju, kako pošiljatelj uočava zagušenje na putu od sebe do odredišta i koji bi algoritam pošiljatelj trebao koristiti da promijeni stopu slanja kao funkciju uočenog zagušenja od kraja do kraja. Može se jednostavno reći da je pošiljateljeva brzina prijenosa broj prenesenih bajtova u sekundi. Prilagođavajući vrijednost poslanih bajtova, pošiljatelj može prilagoditi brzinu kojom se oni šalju u konekciju. Kada postoje prekomjerna zagušenja, onda se jedan ili više usmjerivača na putu preopterećuju uzrokujući da datagram bude odbijen. Odbačeni datagram rezultira gubitkom vremenskog ograničenja. Ako pošiljatelji kolektivno šalju podatke prebrzo, mogu zagušiti mrežu što vodi do kolapsa. Ako su pošiljatelji oprezniji i šalju pakete polako, mogu iskoristiti pojasnu propusnost mreže, odnosno, pošiljatelji bi trebali moći slati na višim stopama bez zagušenja mreže.

5. Pregled programskih alata i sustava za analizu mrežnih protokola

U ovom poglavlju bit će obrađeni programski alati koji se koriste za logičku provjeru mrežnih protokola. Uz samu obradu alata i njihov način rada predstavljeni su i rezultati dobiveni njihovim korištenjem, a to su prikazi protokola korištenih na računalnoj mreži za određene aktivnosti, rezultati skeniranja i hvatanja paketa na mreži, prednosti i nedostaci korištenja svakog od alata, problemi i poteškoće koje se mogu pojaviti na mreži te sumirani prikaz dobivenih rezultata od nekoliko skeniranja u topološkom ili grafičkom obliku. Alati koji su korišteni jesu Wireshark 1.12.2, Softperfect network protocol analyzer 2.9.1 te Zenmap 7.12.

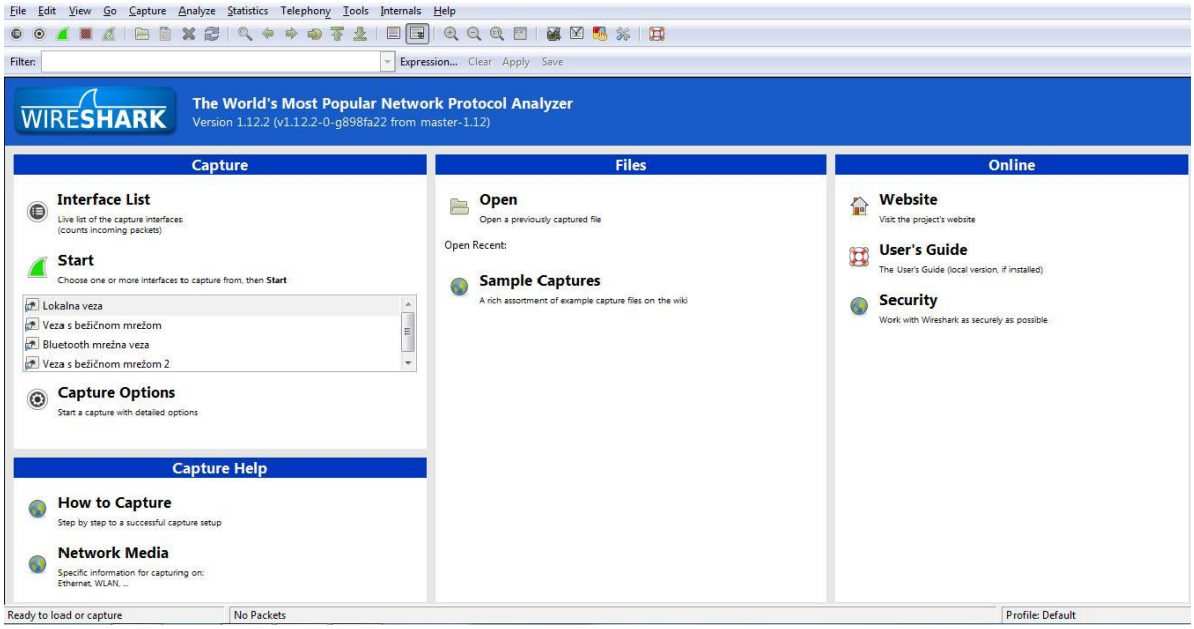
5.1. Wireshark 1.12.2

Najpoznatiji programski alat za analizu mrežnih protokola je Wireshark. Taj programski alat hvata podatke koji u paketima putuju kroz mrežu i prikazuje ih na najdetaljniji mogući način. Alat se koristi za otklanjanje problema na mreži, analizu sigurnosnih ranjivosti, razvoj i implementaciju novih protokola te za učenje o mrežnim protokolima. Osim na OS Windows, Wireshark je moguće pokrenuti i na Unix sustavima kao što su Linux, MAC i Solaris.

Wireshark razumije strukturu mrežnih protokola i iz tog razloga je sposoban prikazati podatke iz paketa koji su specifični za pojedine protokole. Za hvatanje paketa koristi kód *pcap*[16], što znači da može hvatati samo pakete koje *pcap* podržava, a neki od tih su *Ethernet* i IEEE 802.11 [11]. *Pcap* je skup kodova koji raznim programima pružaju programsko sučelje za hvatanje paketa s mreže. Podaci se mogu hvatati izravno s aktivne mrežne veze ili se mogu učitati iz datoteke u kojoj su pohranjeni već uhvaćeni paketi. Dohvaćeni podaci se prikazuju preko grafičkog korisničkog sučelja, a mogu se programski uređivati preko komandne linije ili

[16] Packet capture

pomoću potprograma *editcap*. Alat sadrži i filter za prikaz podataka pomoću kojeg se, ovisno o uvjetima filtriranja, može prikazati i dio podataka.



Slika 6. Početni zaslon alata Wireshark [11]

Početni zaslon sastoji se od padajućih izbornika, glavne trake s prečacima, glavnog prozora, dodatnih alatnih traka te statusne trake (slika 6.).

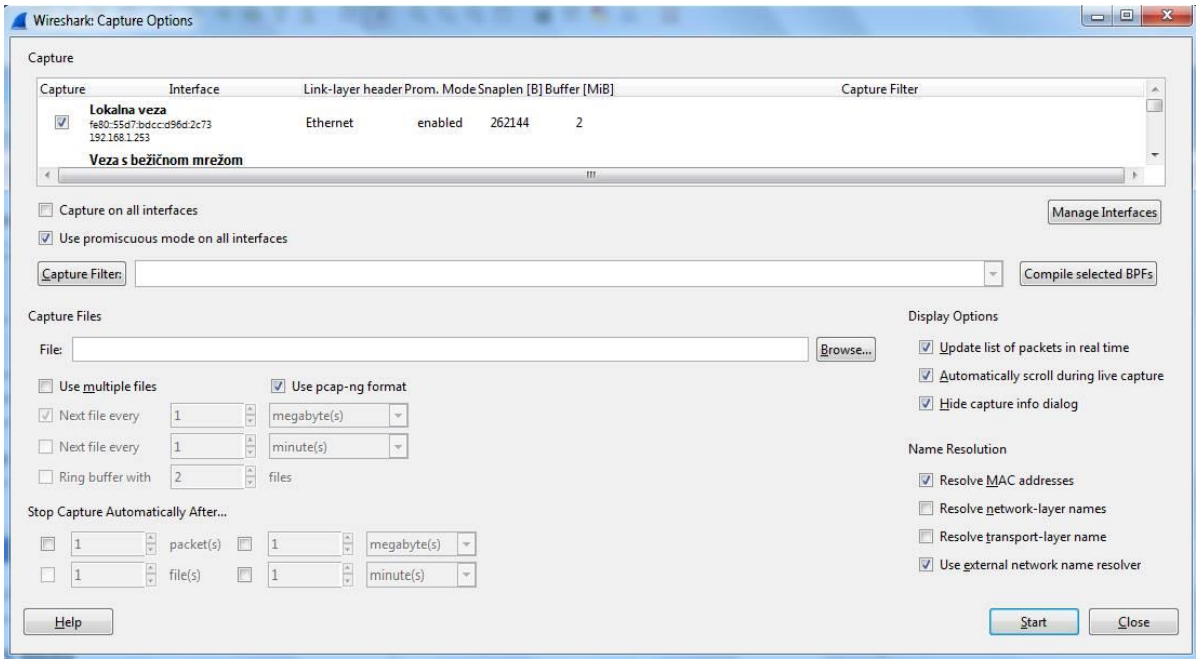
Wireshark se koristi za detektiranje mrežnih problema, proučavanje problema koji se tiču sigurnosti, uklanjanje pogrešaka iz programa nastalih nerazumijevanjem mrežnih protokola te za učenje o mrežnim protokolima [11]. Wireshark nije sustav detekcije upada i ne manipulira stvarima na mreži. Podatke unutar mrežnih paketa može očitati s više mreža, a neke od tih su *Ethernet*, IEEE 802.11, PPP i *Loop-back*. Neke od raširenijih porodica protokola koje se koriste u komunikacijskim mrežama, a koje Wireshark podržava su Internet protokoli, protokoli mobilne telefonije, VOIP protokoli i WAP protokoli. Wireshark sprječava sigurnosne propuste analizom mogućih problema i radnji koje mogu uzrokovati probleme. Zadaci alata se dijele na preventivne i reaktivne. Preventivni zadaci uključuju mrežne metode za očitavanje trenutnog statusa mreže i aplikacije, a koriste se i za uočavanje problema na mreži prije nego što ih korisnik osjeti. Reaktivne metode analize koriste se nakon što greške u radu mreže bivaju uočene. Ukoliko postoji problem s nekim poslužiteljem Wireshark će ga prijaviti

tek nakon što pokuša uhvatiti pakete s mreže. Neke analize koje korisnicima mogu poslužiti u funkciji sigurnosti i administracije mreže su:

- pronalaženje korisnika s najviše prometa na mreži,
- prikaz svih korisnika komunikacijske mreže,
- određivanje mreže ili korisnika koji usporavaju promet na mreži,
- identificiranje asinkronog prijenosa na mreži,
- uočavanje neuobičajenog protokola,
- identificiranje prosječnog i neprihvatljivog vremena odziva mrežnih servisa i mnogi drugi [11].

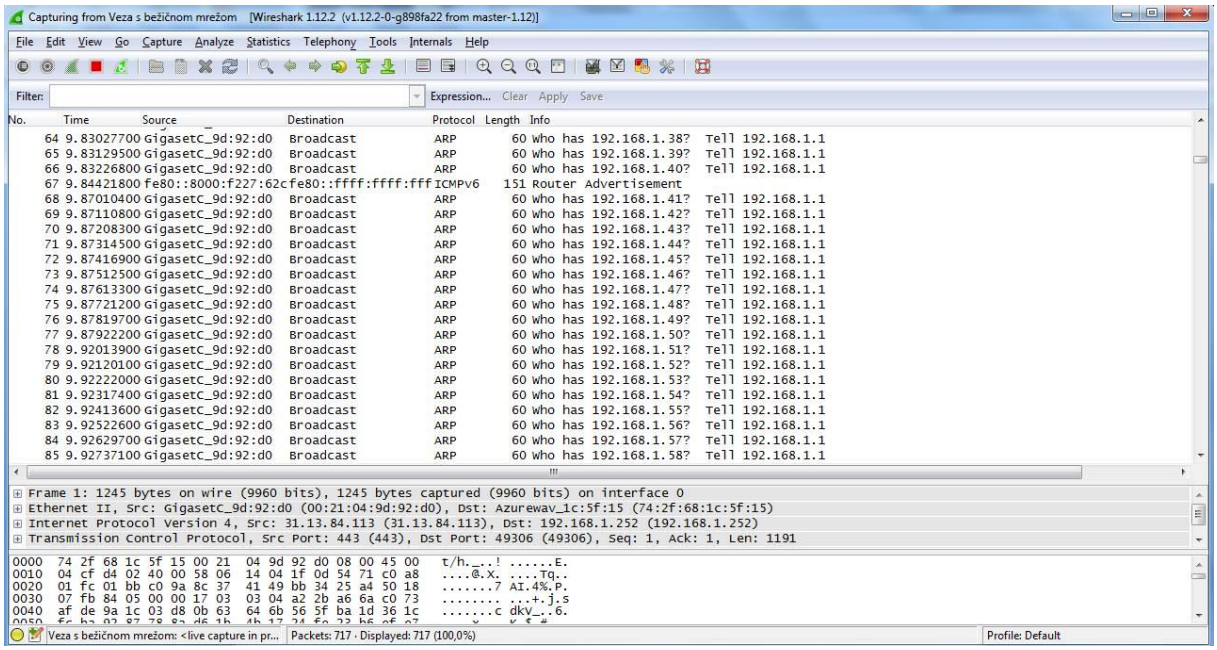
Mogućnosti Wiresharka su hvatanje mrežnih paketa u stvarnom vremenu, uvoz i izvoz te ispis podataka i rad s uhvaćenim paketima. Glavna od tih značajki je hvatanje mrežnih paketa, a omogućuje hvatanje s različitih vrsta mreže, prekid hvatanja uz različite uvjete, simultano prikazivanje dekodiranih istovremeno s hvatanjem novih paketa, filtriranje paketa te reduciranje količine uhvaćenih podataka.

Hvatanje mrežnih podataka u stvarnom vremenu je glavna značajka koja omogućava hvatanje paketa različitih mrežnih tehnologija, zaustavljanje hvatanja paketa definiranjem određenih veličina kao što su vrijeme hvatanja ili količina podataka, simultano prikazivanje dekodiranih paketa bez zaustavljanja aktivnog hvatanja, filtriranje paketa te hvatanje paketa s različitih mrežnih sučelja [9]. Kako bi se pokrenulo hvatanje paketa potrebno je odabrati mrežno sučelje s kojeg će se izvršiti hvatanje paketa i potvrditi tipkom „Start“.



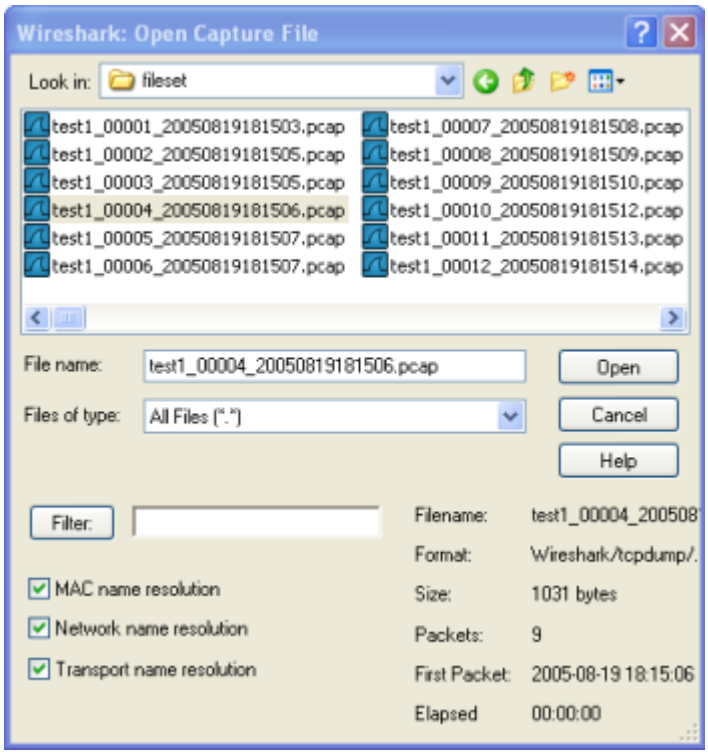
Slika 7. „Capture options“ prozor [11]

Opcija „*capture options*“ sastoji se od šest dijelova. *Capture frame* pokazuje postavke svih dostupnih sučelja, *capture files frame* omogućava da se specificira naziv datoteke koja će se koristiti, *stop capture frame* služi za zaustavljanje postupka hvatanja, *display options frame* ažurira popis paketa u stvarnom vremenu te automatski prebacuje na hvatanje uživo, *name resolution frame* omogućava rezoluciju MAC naziva, mrežnog naziva te transportnog naziva i *buttons* kao posljednji dio daje mogućnost pokretanja ili zaustavljanja nakon što su postavljene željene vrijednosti i odabrane potrebne opcije.



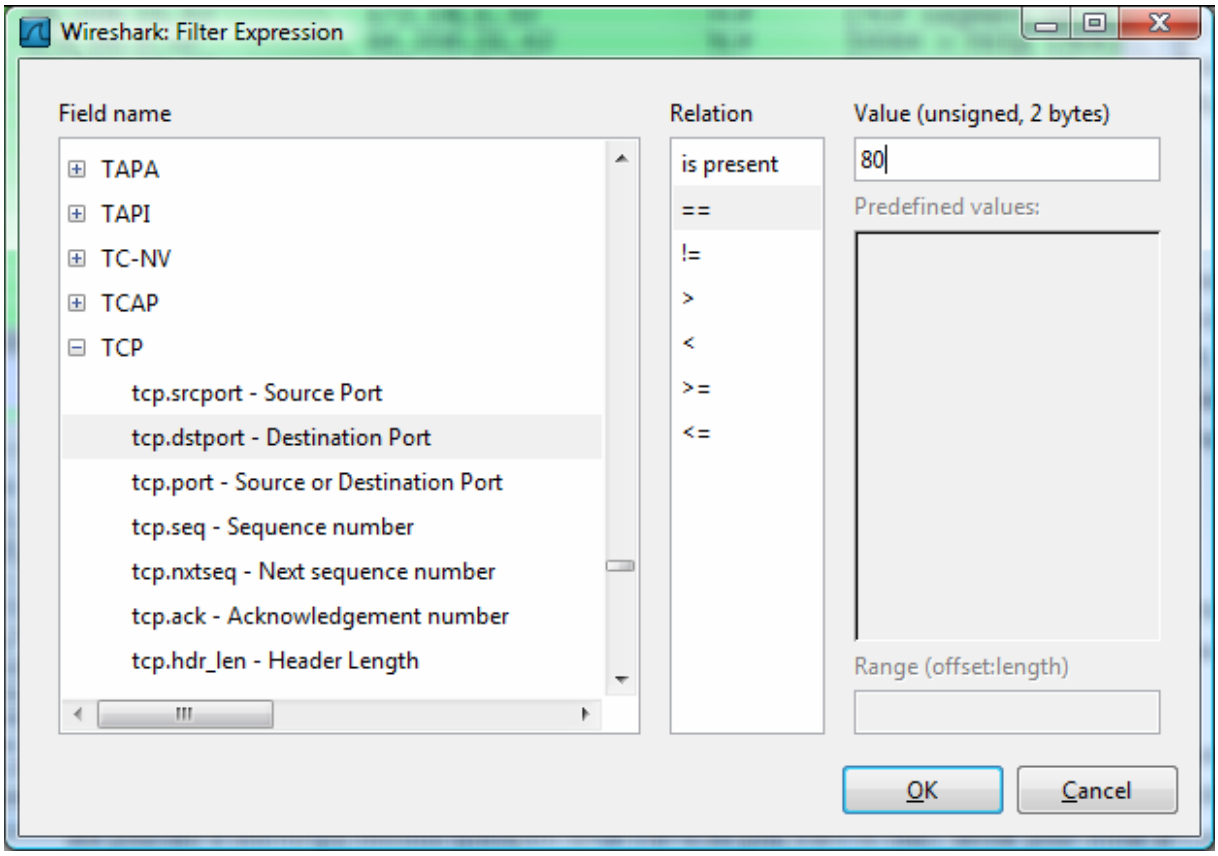
Slika 8. Hvatanje paketa u stvarnom vremenu [11]

Nakon što započne prikupljanje paketa moguće je vidjeti trenutni promet u stvarnom vremenu. Wireshark može i pročitati podatke iz uhvaćenih mrežnih paketa spremljenih u datoteku. Čitanje se obavlja u izborniku „File“ što otvara prozor „Open capture file“.



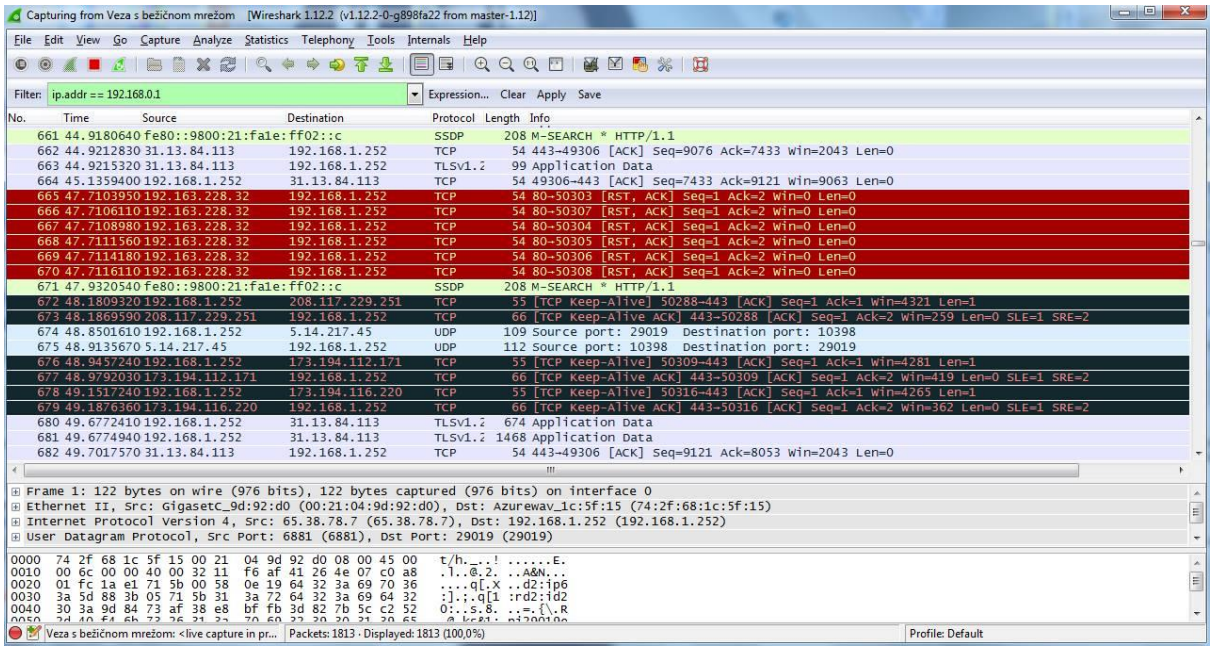
Slika 9. „Open capture file“ prozor [11]

Nakon što završi pokretanje u stvarnom vremenu Wireshark bilježi i ispisuje mrežni promet koji prolazi mrežnim sučeljem. Na slici 9. je prikazano traženje paketa pomoću filtriranja kućnog računala IP adrese 192.168.137.178.



Slika 10. „Filter expression“ [11]

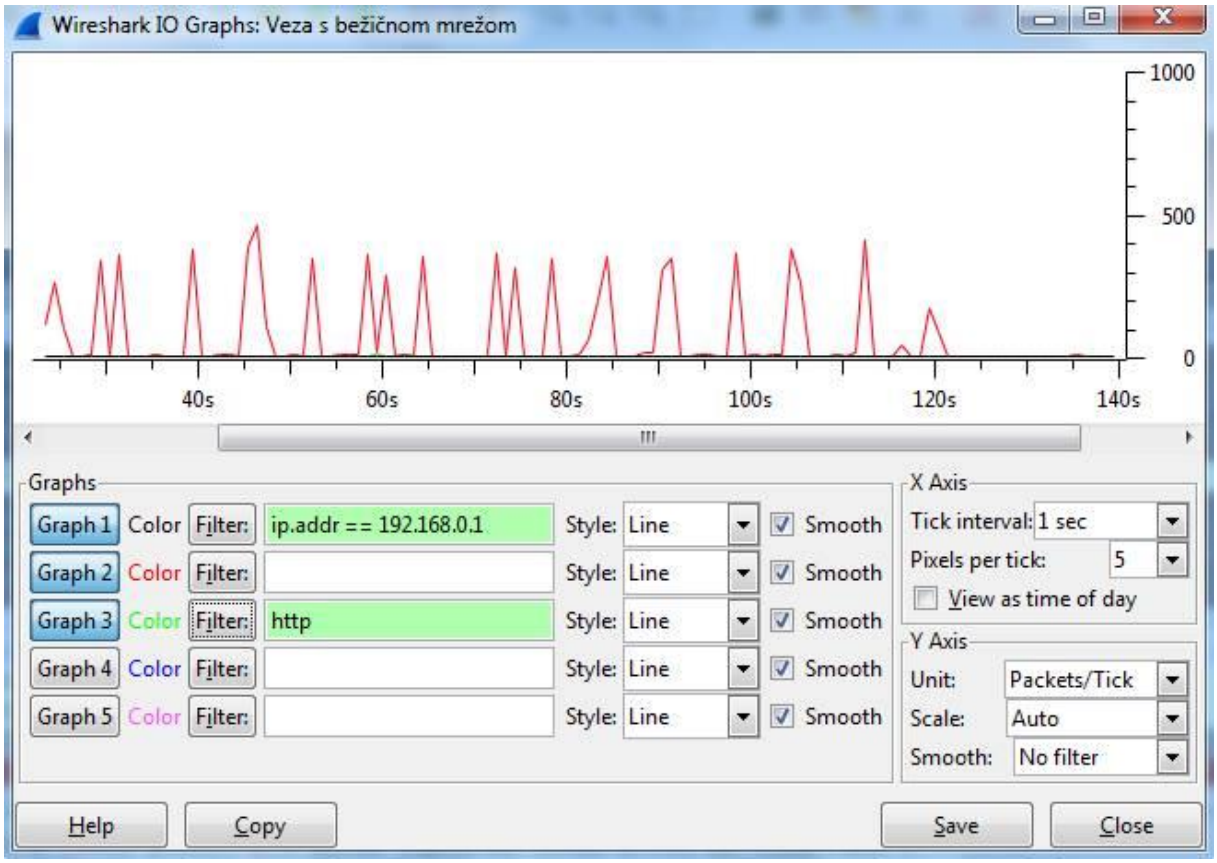
Filter expression može uspoređivati vrijednosti paketa i kombinirati izraze u specifičnije izraze koristeći broj različitih operatora uspoređivanja. Izraze kombinira koristeći logičke operatore I, ILI i NE.



Slika 11. Primljeni i poslani paketi s pripadajućim informacijama [11]

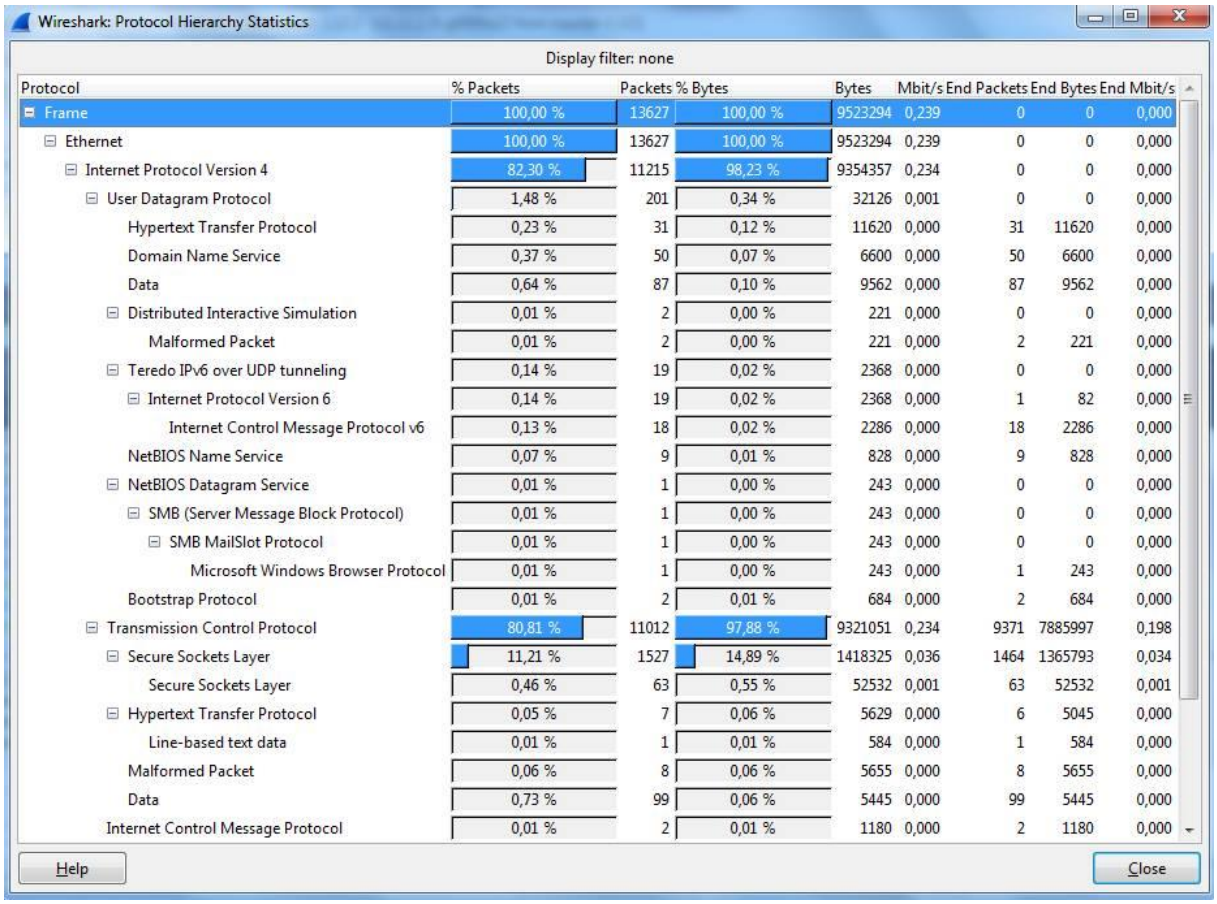
Na slici 11. vidljiv je broj paketa te njihovo vrijeme slanja, izvor i odredište s pripadajućim protokolima te veličina i informacije o paketima. Klikom na pojedini paket moguće je vidjeti detaljan prikaz korištenih protokola, portova, tehnologija prijenosa te sučelja kojima su paketi poslani. Zelenom bojom je označen TCP promet, tamno plavom bojom DNS promet, svijetlo plavom bojom UDP promet i crvenom bojom su označeni TCP paketi s problemima.

Najčešći način izvoza podataka je u ASCII formatu, a izvoz podataka je moguć i u formatima poput PostScript, CSV, PSML te PDML. Moguća je i opcija ispisa paketa što se odabire opcijom „File/print“. Rad s mrežnim paketima obuhvaća prikaz uhvaćenih paketa, njihovo filtriranje, označavanje i ignoriranje. Uhvaćene pakete je moguće filtrirati po mnogim uvjetima te je također moguća izrada vlastitih filtera koji omogućuju selekciju paketa po protokolima, postojanju podataka u paketu, vrijednosti podataka i sličnosti među podacima. Uhvaćeni paketi se mogu i pronaći, a moguće je i označavanje paketa s ciljem isticanja i ignoriranja istih. Wireshark ima i mogućnost statističkog prikaza podataka za pojedini protokol.



Slika 12. Grafički prikaz sumiranog prometa [11]

Za HTTP protokol moguće je izračunati opterećenje po pojedinoj IP adresi, a za TCP protokol je moguće prikazati graf vremena obilaska. Također je moguće vidjeti u kojem su omjeru korišteni pojedini protokoli što je prikazano na slici 13.



Slika 13. Omjer korištenih protokola [11]

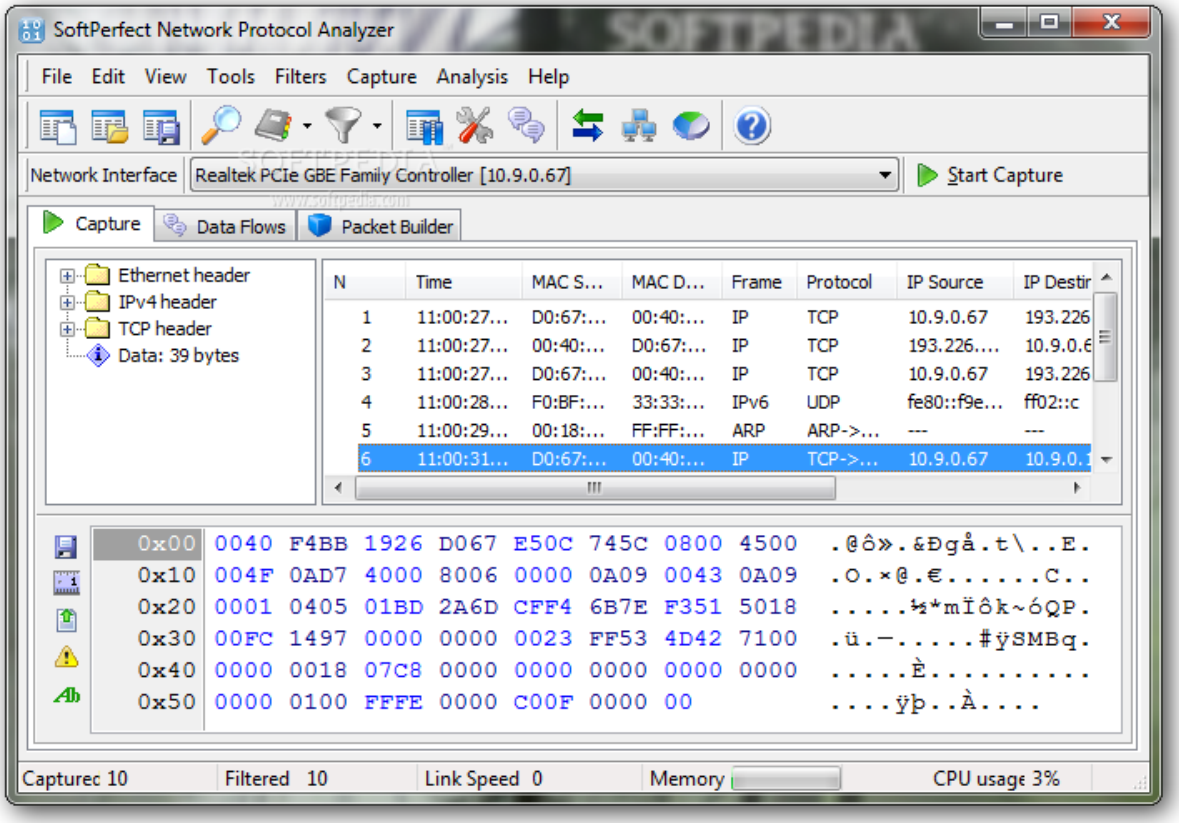
Neke od dodatnih mogućnosti koje nudi ovaj alat su praćenje toka prometa određenog protokola između dvije točke, dekodiranje određenog mrežnog paketa u obliku željenog protokola, prikaz određenog protokola sa specifičnim informacijama te prikaz podataka o greškama i upozorenjima po protokolima.

5.2. Softperfect network protocol analyzer 2.9.1

Drugi važan alat je Softperfect network protocol analyzer. To je besplatni profesionalni alat za analizu, ispravljanje pogrešaka te za održavanje i nadzor lokalnih mreža i internetske mreže. On hvata podatke koji prolaze *dial-up*[17] konekcijom ili

[17] Način pristupa Internetu pri čemu se koriste modem i telefonska linija

Ethernet mrežnom karticom, analizira ih i predstavlja u čitljivom obliku. Alat je koristan za administratore mreže, sigurnosne stručnjake, programerima mrežnih aplikacija te svakome tko treba cjelovitu sliku prometa koji prolazi kroz njihovu mrežnu vezu ili segment lokalne mreže [17]. Alat prikazuje rezultate analize u prikladnom i lako razumljivom formatu. Može defragmentirati i ponovno sastavljati pakete. Također ima mogućnost punog dekodiranja i analizu mrežnog prometa baziranom na protokolima poput ARP, ICMP, IGMP, IP, RIP, TCP i UDP. Obavlja i rekonstrukciju vršnih protokola poput HTTP, SMTP, POP, IMAP i FTP.

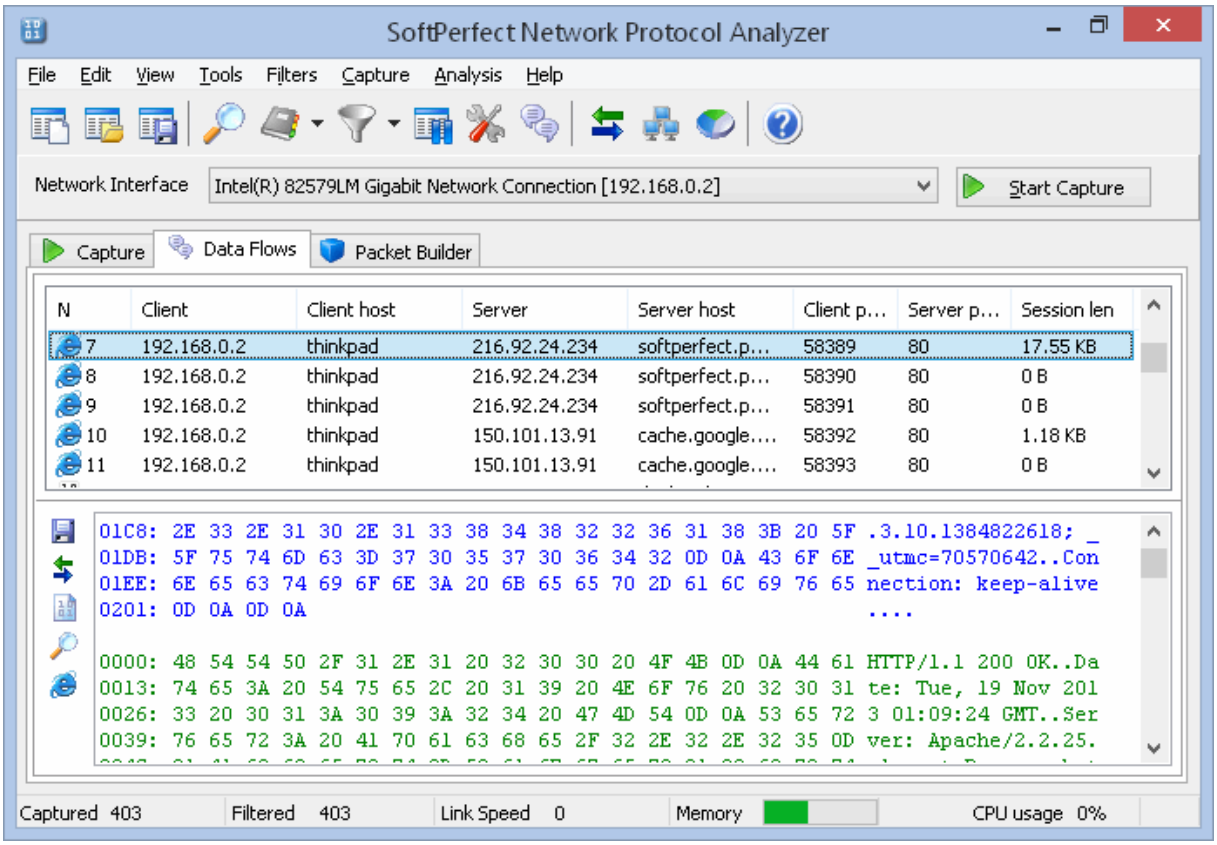


Slika 14. Paketi uhvaćeni s LAN-a [17]

Alat se može koristiti za odbacivanje svog mrežnog prometa, osim određenog kojeg korisnik želi analizirati, a ima i mogućnost građenja paketa što omogućava izgradnju vlastitih prilagođenih mrežnih paketa i njihovo slanje na mrežu. Graditelj paketa može se

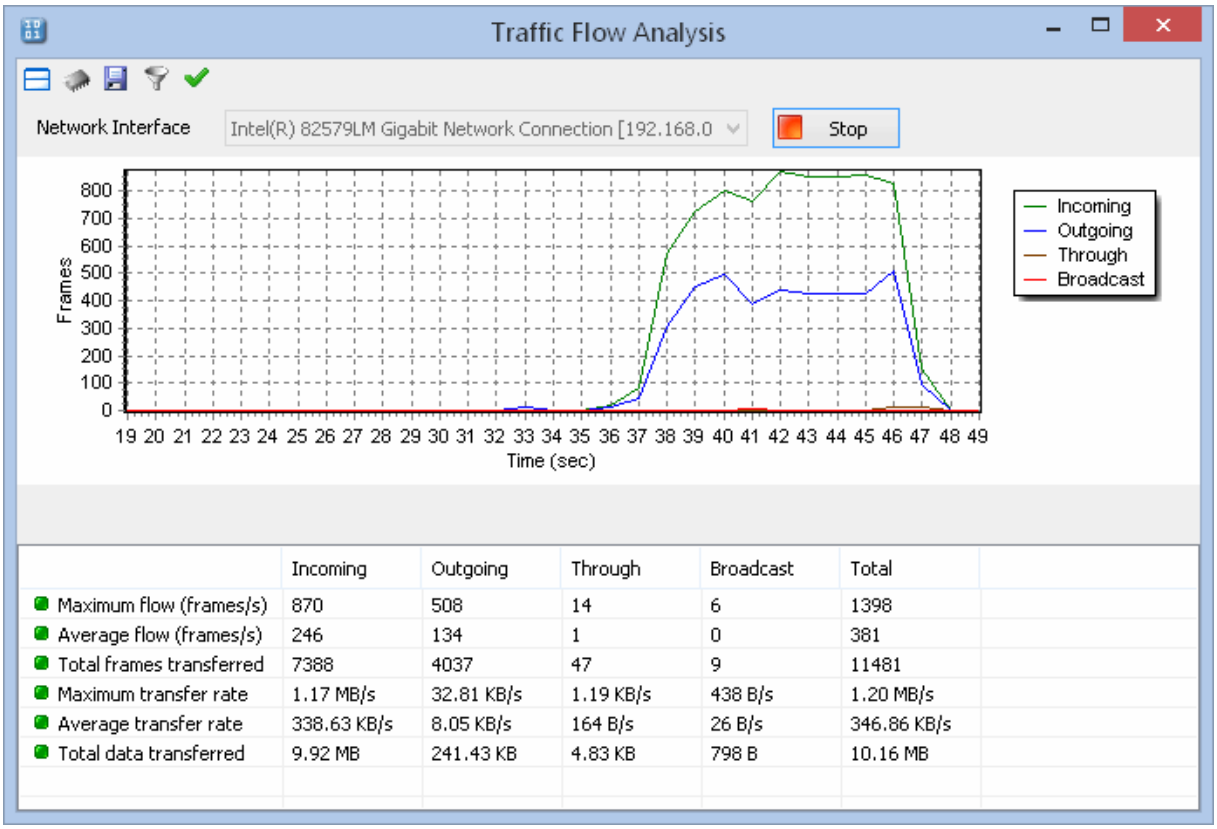
koristiti i za provjeru mrežne zaštite od napada i uljeza. Neke od glavnih značajki ovog alata su:

- dekodiranje paketa i njihov prikaz u čitljivom formatu,
- mogućnost izgradnje vlastitih paketa i slanje istih na mrežu,
- rad u miješanom modu za hvatanje svih mrežnih paketa,
- nuđenje fleksibilnog prometnog filtriranja,
- rekonstruiranje paketa u tokove te
- praćenje neuspjelih pokušaja ostvarivanja veze unutar sustava [17].



Slika 15. Uhvaćena i rekonstruirana HTTP sesija prikazana u heksadecimalnom obliku [17]

Na slici 15. vidljiv je klijentsko-serverski odnos s podacima o mrežnom sučelju, IP adresama te broju uhvaćenih i filtriranih paketa.

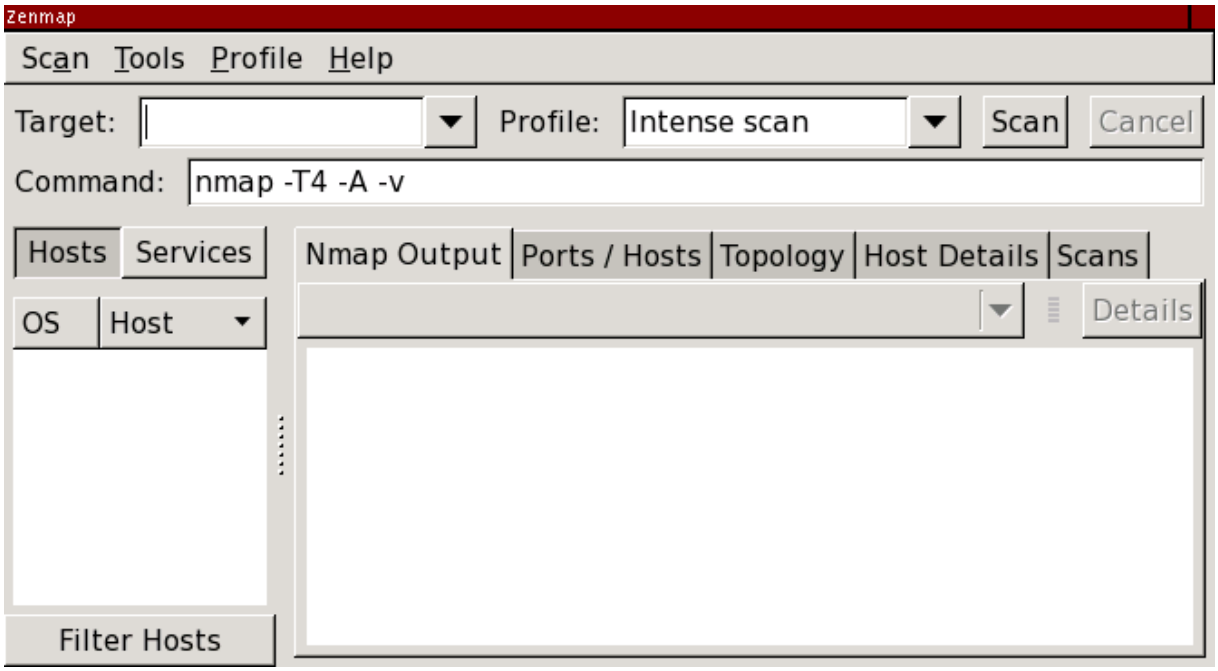


Slika 16. Analiza prometnog toka [17]

Na slici 16. prikazana je kompletna analiza prometnog toka nakon završenog skeniranja mrežnog sučelja s pripadajućim vrijednostima te dijagramom.

5.3. Zenmap 7.12

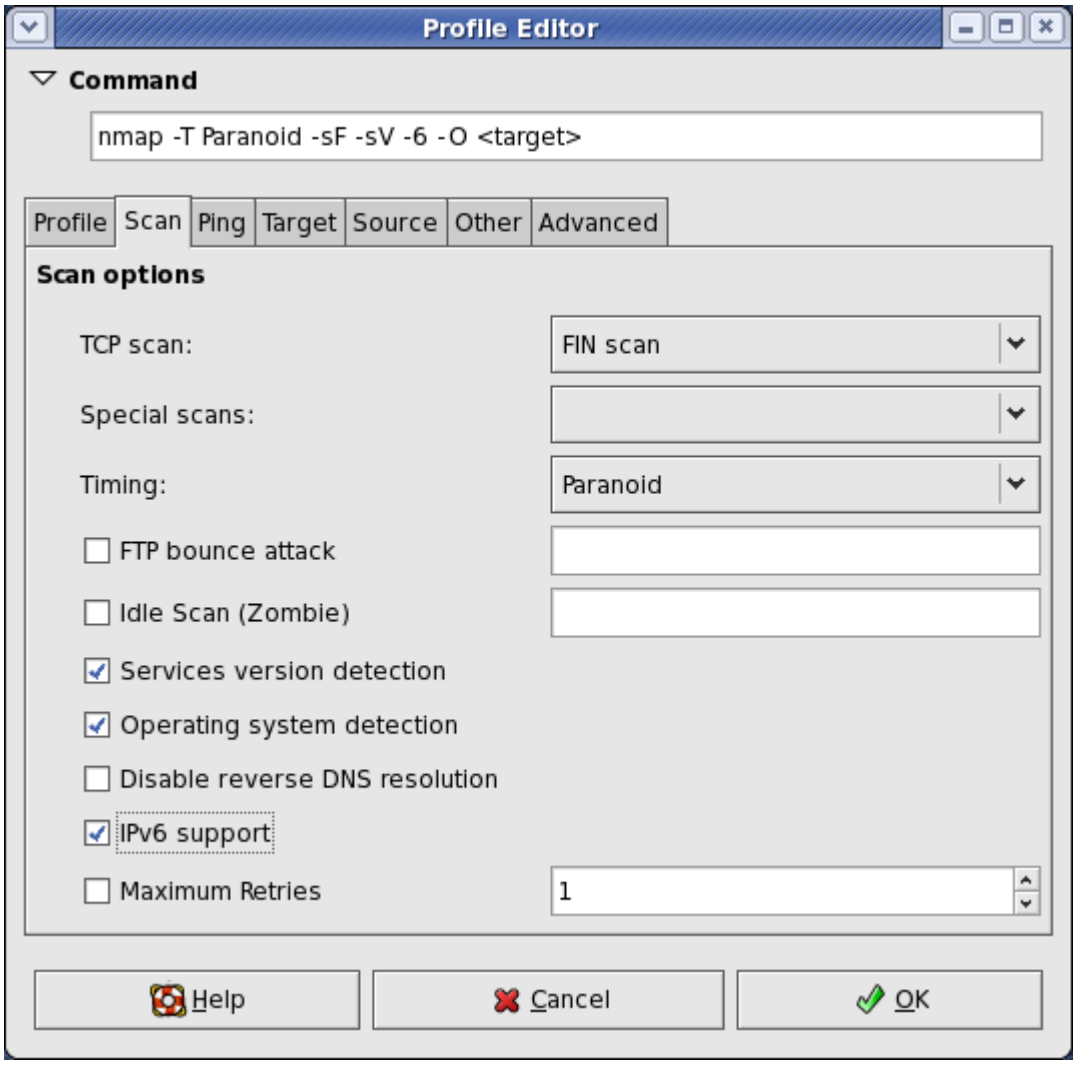
Idući od alata za provjeru protokola je Zenmap. To je službeni GUI alata Nmap, besplatan je i ima za cilj da Nmap alat učini lakim za korištenje početnicima, a pruža napredne mogućnosti za iskusne korisnike [14]. Stalno korištena skeniranja mogu biti sačuvana kao profili kako bi se mogli pokrenuti više puta za redom. Naredba „Creator“ omogućava interaktivno kreiranje komandnih linija. Rezultati skeniranja mogu se sačuvati i kasnije pregledavati. Također se mogu uspoređivati jedan s drugim kako bi se vidjela razlika među njima. Rezultati nedavnih skeniranja pohranjuju se u bazu podataka.



Slika 17. Početni prozor alata Zenmap [14]

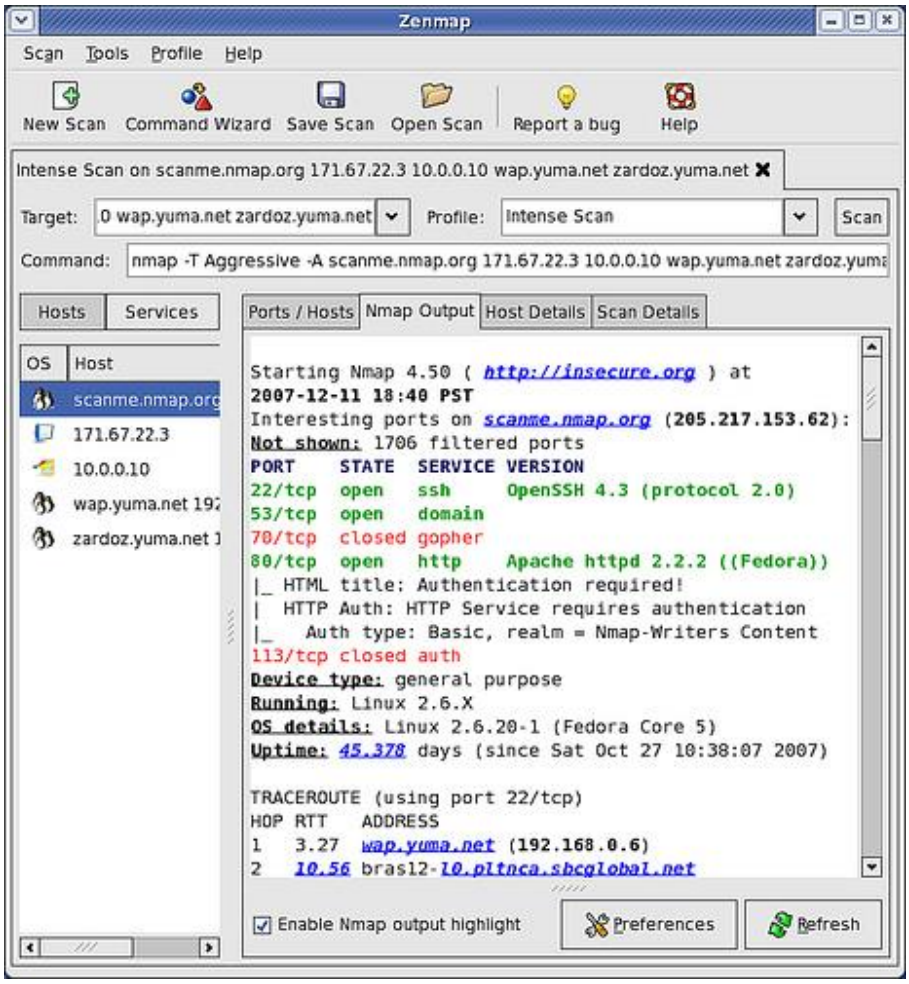
Prednosti koje ovaj alat pruža su:

- organiziranje zaslona za prikaz svih portova na računalima pojedine usluge,
- pokazivanje razlike između dvaju skeniranja,
- praćenje rezultata skeniranja dok ih korisnik ne odluči odbaciti te
- mogućnost pokretanja istog skeniranja više od jednom [14].



Slika 18. Zenmap kreiranje profila [14]

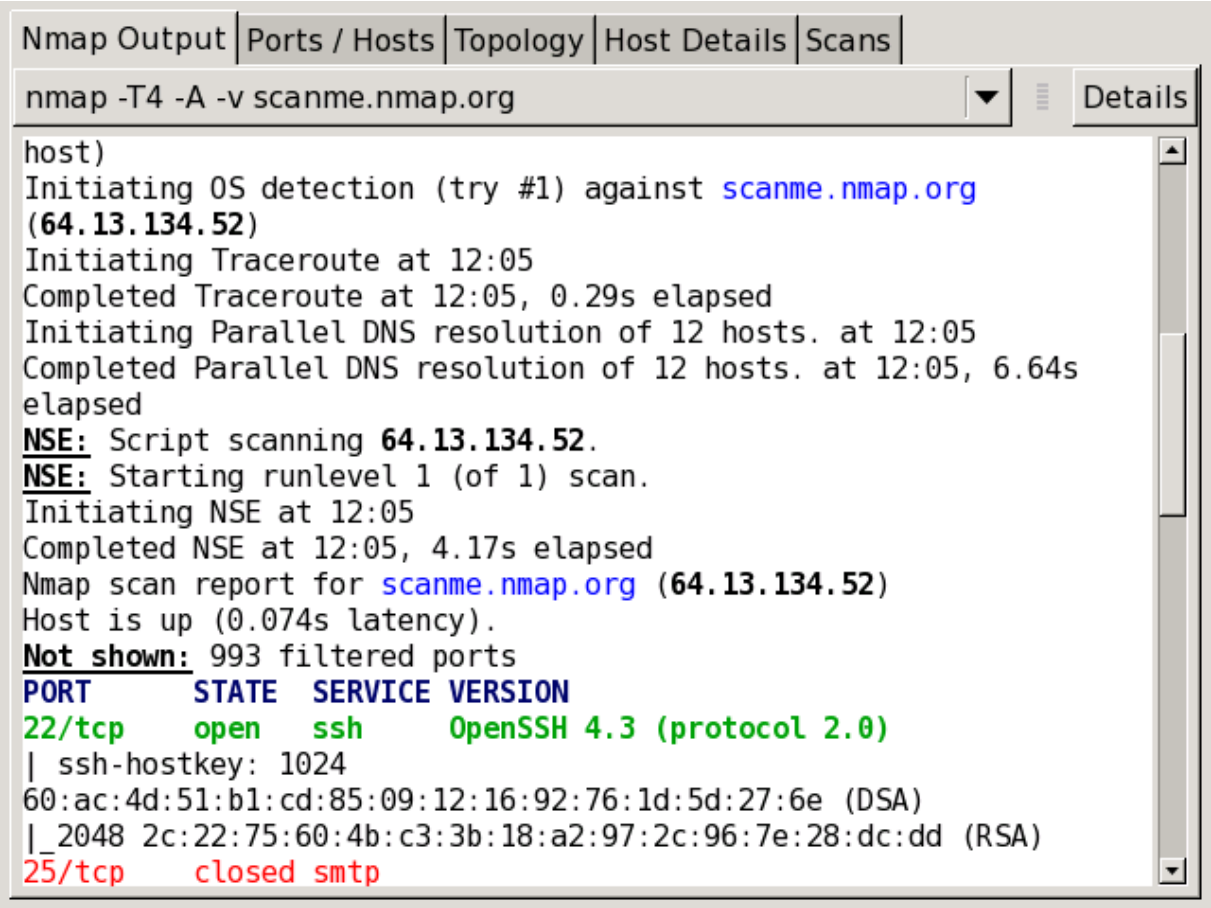
Organiziranjem zaslona sažima podatke o *hostu* ili o kompletnom skeniranju u praktičan prikaz. Može prikazati topološku mapu otkrivenih mreža. Rezultati nekoliko skeniranja mogu se kombinirati i pregledati odjednom. Pokazivanjem razlike između dvaju skeniranja moguće je vidjeti što se promijenilo u jednom skeniranju pokrenutom u različitim danima, između skeniranja dvaju različitih *hostova* te između skeniranja istog *hosta* s drugačijim postavkama. Ovo administratorima omogućava praćenje novih *hostova* ili servisa koji se pojavljuju na mrežama. Moguće je pokrenuti skeniranje, vidjeti rezultate, a potom odlučiti hoće li oni biti spremljeni u datoteku.



Slika 19. Detalji skeniranja [14]

Skeniranje se pokreće upisivanjem naredbe „scanme.nmap.org“ u polje „Target“, odabirom profila „Intense scan“ i klikom na tipku „Scan“. Intenzivno skeniranje je jedna od mogućnosti skeniranja. Profil je moguće odabrati za više vrsta skeniranja, a nakon odabira na ekranu se prikazuje komandna linija povezana s profilom. Profile je moguće uređivati i stvarati nove što se nalazi u sekciji „The profile editor“. Ovaj alat ima mogućnost kombiniranja više rezultata mnogih skeniranja u jedan pregled što se naziva „agregacija skeniranja“. Nakon što završi jedno skeniranje, moguće je u istom prozoru započeti drugo. Kad završi drugo skeniranje, rezultati se spajaju s prvim skeniranjem, a njihova zbirka koja čini skupni pregled se zove mrežni inventar. Nije neophodno čekati da se skeniranje završi kako bi se započelo drugo skeniranje, nekoliko skeniranja se može obavljati uzastopno. Prilikom završetka bilo kojeg od skeniranja, rezultati se dodaju u zajednički inventar. Također je moguće imati otvoreno više od jednog inventara istovremeno, potrebno je samo iz

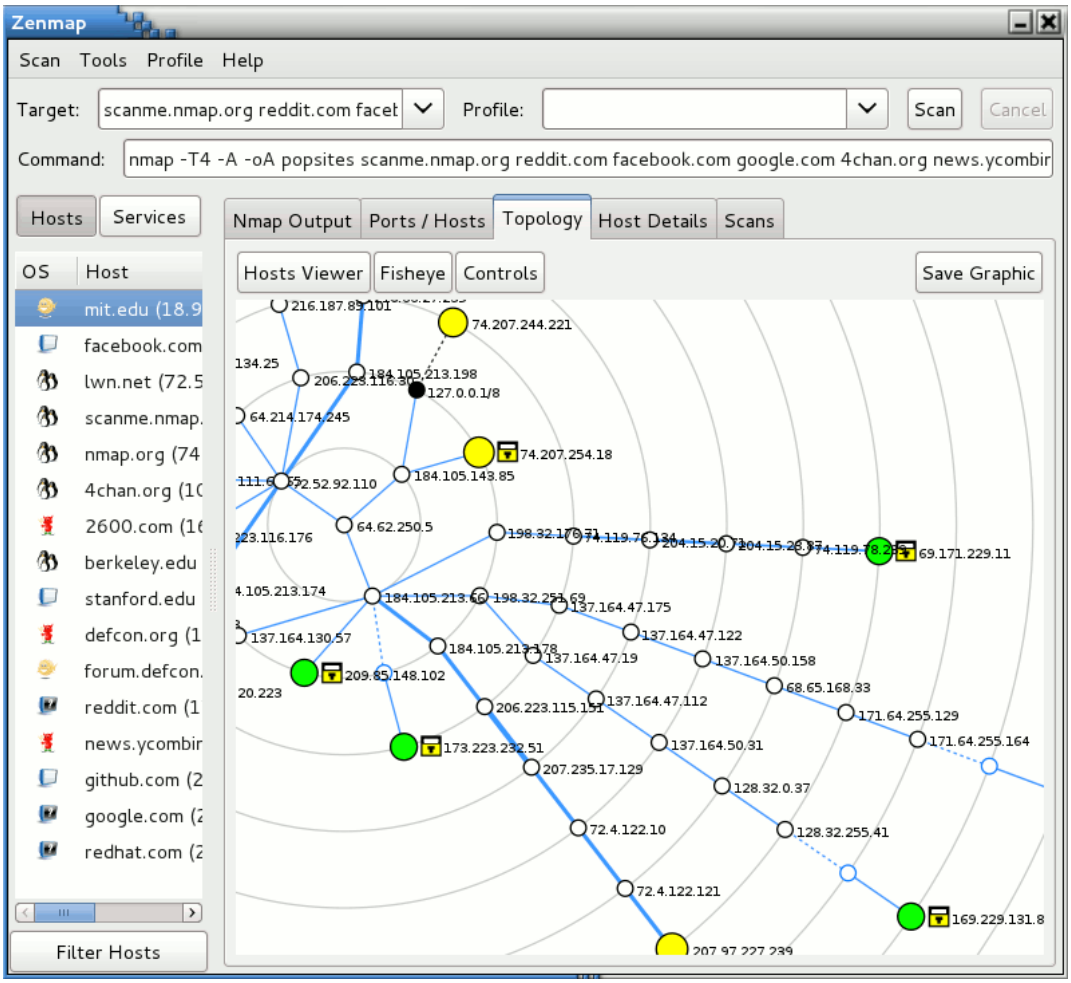
izbornika „Scan“ odabrati „New window“ ili kombinacijom tipki *ctrl+N*. Rezultati skeniranja prikazuju se za vrijeme i nakon skeniranja i to na način koji te rezultate čini jednostavnima za razumijevanje i korištenje. Svaki prozor skeniranja sadrži pet kartica od kojih svaka prikazuje različite aspekte skeniranja. Te kartice su „Output“, „Ports/hosts“, „Topology“, „Host details“ te „Scans“.



Slika 20. Kartica „Output“ [14]

Kartica se prikazuje po zadanim postavkama dok traje skeniranje, a prikazuje poznate terminalne izlaze. Na zaslonu su istaknuti dijelovi u skladu s njihovim značenjem pa su tako otvoreni i zatvoreni portovi prikazani u različitim bojama. „Ports/hosts“ tablica se razlikuje ovisno o tome je li označen *host* ili usluga. Kada je označen *host*, prikazani su svi portovi na njemu zajedno s informacijom o verziji, ako je dostupna. Kada je označena usluga prikazuju se svi *hostovi* koji pojedini port imaju otvoren ili filtriran. „Topology“ kartica je prikaz veza

između *hostova* na mreži. *Hostovi* su povezani u koncentričnim krugovima. Svaki prsten predstavlja dodatni mrežni skok iz središnjeg čvora.

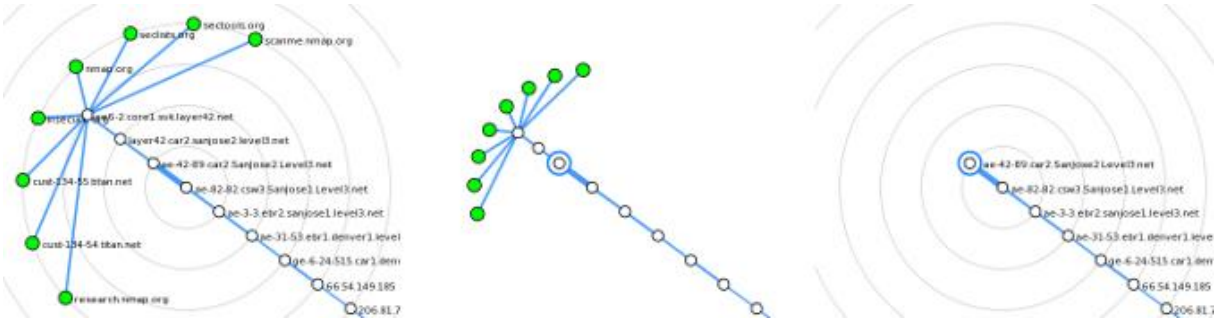


Slika 21. Prikaz topologije *hostova* na mreži [14]

Ta kartica pruža interaktivnu vizualizaciju veza između *hostova* na mreži. *Hostovi* su prikazani kao čvorovi na grafu koji se radijalno proteže od središta. Zaslon je moguće micati, a klikom na neki od *hostova*, on postaje novi centar. Graf se automatski preslaguje i prikazuje novi izgled topologije, a pokretanjem novog skeniranja svaki novi *host* ili mrežni put se automatski dodaju na topologiju. Pogled topologije je najkorisniji kada se koristi opcija „Traceroute“ iz razloga što ona otkriva mrežni put prema *hostovima*.

Također je moguće i podešavanje kontrola koje klikom na pojedini *host* prikazuju što se s njima događa. Postoje 4 grupe kontrola, a to su „Change focus“ koja omogućava

preraspodjelu *hostova* radi postavljanja određenog *hosta* u centar, „Show information“ za prikaz informacija o *hostovima*, „Group children“ za spajanje čvorova u jednu grupu te „Fill region“ za označavanje područja u kojem su čvorovi spojeni u grupu.



Slika 22. Grupiranje čvorova [14]

Druga skupina kontrola je interpolacija koja određuje koliko se brzo animacija nastavlja kada se dio grafa promijeni. Kartica „Host details“ prikazuje sve informacije o pojedinom *hostu* u hijerarhijskom prikazu, a to su njihova imena i adrese, stanje te broj i status skeniranih portova. Kartica „Scans“ prikazuje sva skeniranja koja se prikupljaju kako bi se načinio mrežni inventar. Iz te kartice je moguće dodavanje i micanje skeniranja, a klikom na „Cancel scan“ moguće je prekinuti trenutno skeniranje.

6. Komparativna analiza programskih alata i sustava za analizu mrežnih protokola

Svi programski alati navedeni u prethodnom poglavlju razlikuju se po više kriterija jedan od drugoga. Ono što je najbitnije razlikovati jesu njihove funkcije koje oni mogu obavljati. Svaki alat može obavljati neke funkcije koje drugi nije u mogućnosti odraditi. Primjerice, Wireshark i Softperfect network protocol analyzer imaju, osim hvatanja i analize paketa, mogućnost uočavanja problema i pogrešaka na mreži koje oni sami, bez potrebe korištenja drugih alata, mogu i ispraviti dok Zenmap služi isključivo za njuškanje i analizu protokola korištenih na mreži. Ovo ne predstavlja problem jer alat Zenmap služi korisnicima kako bi saznali strukturu i informacije o protokolima korištenima na određenim dijelovima mreže, a pogreške ne uočavaju pa korisnici ne mogu ni znati postoji li pogreška ili problem. Ta dva alata koriste isključivo oni korisnici kojima je u cilju saznati što više informacija o strukturi pojedinih protokola. Ukaže li se potreba ili namjera za otkrivanjem pogrešaka na mreži, s razlogom saznanja koji protokoli su najpouzdaniji i koji se protokoli na mreži najčešće pojavljuju s problemima, tada se koriste Wireshark i Softperfect network protocol analyzer.

Wireshark nudi mogućnost implementacije novih protokola, a ne samo analize postojećih kao i mogućnost učenja o protokolima koji korisnicima možda predstavljaju nepoznanicu dok ostali alati te mogućnosti nemaju. Ovo je dobra prednost alata Wireshark jer na taj način i početnici mogu savladati korištenje alata. Wireshark također ima mogućnost provjere broja korisnika koji se nalaze na mreži i na taj način može odrediti usporenost prometa na mreži i identificirati srednje vrijeme odziva mrežnih servisa. Također, jedna od razlika je ta što ga je, osim na OS Windows, moguće pokrenuti i na Linux, MAC i Solaris operacijskim sustavima.

Softperfect network protocol analyzer hvata isključivo one podatke koji prolaze *dial-up* konekcijom ili *Ethernet* mrežnom karticom. Ima mogućnost izgradnje vlastitih paketa i slanje istih na mrežu, dok Wireshark ima samo mogućnost implementacije novih protokola. Jedna od značajki ovog alata koju drugi alati ne podržavaju je ta što može pratiti neuspjele pokušaje ostvarivanja veza između sustava.

Prednosti koje Zenmap pruža, a po kojima se razlikuje od ostalih alata su mogućnost pokretanja više od jednog skeniranja istovremeno i mogućnost sumiranja rezultata odvojenih skeniranja u jedan inventar i njihova međusobna usporedba. Svaki od alata ima mogućnost prikaza topologije rezultata skeniranja, a ono po čemu se Zenmap razlikuje od ostalih u tome je to što se pokretanjem novih skeniranja i hvatanja paketa rezultati automatski dodaju na topološki prikaz i mogućnost pregleda topologije po određenom *hostu* koji se može postavljati kao središnji, a ostali *hostovi* se prilagođavaju njemu i automatski rade preraspodjelu topologije.

Tablica 1. Komparativna analiza programskih alata

Programski alat	*Wireshark*	*Softperfect*	*Zenmap*
Funkcije	- Hvatanje i analiza paketa - Mogućnost uočavanja pogrešaka - Implementacija novih protokola	- Hvatanje i analiza paketa - Mogućnost uočavanja pogrešaka - Izgradnja vlastitih paketa	- Sadrži informacije o strukturi protokola - Mogućnost usporedbe rezultata
Glavne prednosti	- Mogućnost implementacije novih protokola - Mogućnost provjere broja korisnika na mreži	- Mogućnost praćenja neuspjelih pokušaja ostvarivanja veza između sustava	- Mogućnost pokretanja više od jednog skeniranja istovremeno
Zajednička funkcija	- Prikaz topologije rezultata skeniranja	- Prikaz topologije rezultata skeniranja	- Prikaz topologije rezultata skeniranja

U tablici 1. prikazana je usporedba programskih alata prema glavnim značajkama, prednostima i zajedničkoj funkciji. U prvom redu su navedene funkcije koje obilježavaju pojedini programski alat. U drugom redu su navedene glavne prednosti svakog alata,

odnosno prednosti koje svaki alat ima u odnosu na druge, a u trećem redu je navedena funkcija koja je zajednička svakom alatu.

7. Zaključak

Internet je danas dio svakodnevice i postalo je uobičajeno da ga se koristi u svakodnevnim djelatnostima. Kao i svako drugo sredstvo informacija ili pak pomagalo pri radu, nužno je da njegov rad bude brz, efikasan i djelotvoran kako bi njegova upotreba bila od nekog značenja. Ono što pomaže u radu Interneta su mrežni protokoli raspoređeni po njegovim slojevima od kojih svaki ima svoju funkciju, neki veću, a neki pak manju, ali svi protokoli međusobno potpomažu lakom i brzom korištenju Interneta. Protokoli mogu ostvarivati siguran prijenos podataka, prenositi podatke ili ih kodirati. Svaki od protokola na pojedinom sloju se međusobno razlikuje, imao on istu namjenu kao drugi protokoli ili ne, jer svakoj određenoj radnji odgovara i određeni protokol.

Kako bi se njihovo korištenje, funkcije, prednosti i nedostaci te međusobne usporedbe lako mogli proučavati koriste se određeni alati koji obavljaju logičku provjeru tih protokola. Logička provjera prikazuje i opisuje koji su se protokoli koristili na mreži za vrijeme obavljanja određenih funkcija. Osim logičke provjere, protokoli se i istražuju s ciljem zadržavanja važnosti softvera ili s ciljem izgradnje učinkovite implementacije protokola. Logikom za dokazivanje sigurnosnih svojstava protokola moguće su operacije poput dešifriranja ili verifikacije, a rezultati toga su kompozicijski teoremi i računalna ispravnost istih.

Pomoću alata moguće je ustanoviti koji se protokoli koriste točno na kojem dijelu mreže te je li njihova upotreba pouzdana ili nije. Moguće je ispravljanje pogrešaka ukoliko one postoje te razvoj novih protokola uz samu mogućnost korištenja postojećih. Protokoli se mogu detaljno proučavati te se rezultati hvatanja paketa na mreži mogu sumirati u jednu bazu kako bi se dobio strukturiran prikaz uhvaćenih paketa u jednoj sesiji.

Analizirani programski alati dobro su osmišljeni, jednostavni su za korištenje te pružaju točne i relevantne informacije o mrežnom sučelju te njegovim protokolima. Alati imaju mogućnost brzog pregleda rezultata dobivenih skeniranjem mreže te mogućnost uvida u pogreške koje se na mreži javljaju.

Programski alati se svakodnevno usavršavaju i unaprjeđuju kako bi korisnicima rad s istima bio što lakši i praktičniji pri skeniranju mrežnih protokola odnosno analizi mrežnih podataka te kako bi u budućnosti rezultati skeniranja davali još više podataka i informacija o mrežnom sučelju, a samim time i što detaljniju sliku mrežne strukture.

Literatura

[1] http://www.bug.hr/forum/topic/internet/uvod-mrezne-protokole/96549.aspx (Kolovoz, 2017.)

[2] http://tfotovic.tripod.com/ni_protokoli.htm (Kolovoz, 2017.)

[3] http://www.informatika.buzdo.com/pojmovi/tcp-ip-1.htm (Kolovoz, 2017.)

[4] http://www.informatika.buzdo.com/s430-osi-model.htm (Kolovoz, 2017.)

[5] http://www.cis.hr/files/dokumenti/CIS-DOC-2011-02-004.pdf (Kolovoz, 2017.)

[6] https://sysportal.carnet.hr/node/352 (Kolovoz, 2017.)

[7] https://support.microsoft.com/en-us/kb/103884 (Kolovoz, 2017.)

[8] http://searchnetworking.techtarget.com/answer/What-is-the-difference-between-OSI-model-and-TCP-IP-other-than-the-number-of-layers (Kolovoz, 2017.)

[9] http://searchnetworking.techtarget.com/definition/TCP-IP (Kolovoz, 2017.)

[10] http://marjan.fesb.hr/~julije/purm/uorm.pdf (Kolovoz, 2017.)

[11] http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-09-312.pdf (Kolovoz, 2017.)

[12] https://sourceforge.net/projects/nast.berlios/ (Kolovoz, 2017.)

[13] https://lists.nongnu.org/archive/html/slackit-ml/2003-01/msg00031.html (Kolovoz, 2017.)

[14] https://nmap.org/zenmap/ (Kolovoz, 2017.)

[15] https://nmap.org/book/zenmap.html (Kolovoz, 2017.)

[16] http://www.veleri.hr/files/datoteke/page_privitak/Zavrsni_rad_baric_final.pdf (Kolovoz, 2017.)

[17] https://www.softperfect.com/products/networksniffer/ (Kolovoz, 2017.)

[18] http://www.usconverters.com/index.php?main_page=page&id=61 (Kolovoz, 2017.)

[19] https://en.wikipedia.org/wiki/IPv6 (Kolovoz, 2017.)

[20] http://www.serv-u.com/ftp-server-setup-windows (Kolovoz, 2017.)

[21] http://www.techrepublic.com/blog/five-apps/five-free-network-analyzers-worth-any-it-admins-time/ (Kolovoz, 2017.)

[22] Belov, M.; „Programming and formal verification of network communication protocols implementations“ – Birkbeck, University of London, Department of Computer science and information systems, 2012. (Kolovoz, 2017.)

[23] Datta, A., Derek A., Mitchell J.C., Roy A.; „Protocol composition logic (PCL)“ – Computer science department-Stanford university-Stanford, 2007. (Kolovoz, 2017.)

[24] http://seclab.stanford.edu/pcl/ (Kolovoz, 2017.)

[25] Bharti, V., Kumar S.; „Survey of network protocol verification techniques“ – AKG Engineering College, Gzb, India, 2012. (Kolovoz, 2017.)

[26] Kurose, J.F., Ross K.W.; „Computer networking – A top-down approach“ – University of Massachusetts, Amherst, 2013. (Kolovoz, 2017.)

[27] https://mreze7bd.wikispaces.com/Mre%C5%BEni+protokoli (Kolovoz, 2017.)

Popis kratica i akronima

Kratica	Značenje	Kratica	Značenje
ARP	Address resolution protocol	NFS	Network file system
ASCII	American standard code for information interchange	NNTP	Network news transfer protocol
ATM	Asynchronous transfer mode	NTP	Network time protocol
CRC	Cyclic redundancy check	OSI	Open systems interconnection
CSMA/CD	Carrier-sense multiple access with collision detection	POP	Post office protocol
DCAP	Dependent care assistance program	PPP	Point-to-point protocol
DCCP	Datagram congestion control protocol	PPTP	Point-to-point tunneling protocol
DHCP	Dynamic host configuration protocol	PVC	Private virtual channel
DNS	Domain name system	RARP	Reverse address resolution protocol
EBCDIC	Extended binary coded decimal interchange code	RIP	Routing information protocol
FDDI	Fiber distributed data interface	SAP	Service advertising protocol

FEC	Forward error correction	SCTP	Stream control transmission protocol
FTP	File transfer protocol	SIP	Session initiation protocol
HTML	Hypertext markup language	SMPP	Short message peer-to-peer
HTTP	Hyper text transfer protocol	SMTP	Simple mail transfer protocol
ICMP	Internet control message protocol	SNMP	Simple network management protocol
IEEE	Institute of electrical and electronics engineers	TCP/IP	Transmission control protocol/Internet protocol
IGMP	Internet group management protocol	TDI	Transport driver interface
L2TP	Layer 2 tunneling protocol	UDP	User datagram protocol
LAN	Local area network	WAN	Wide area network
LLC	Logical link control	WAP	Wireless application protocol
MAC	Media access control	WIFI	Wireless fidelity
MIDI	Musical instrument digital interface	WLAN	Wireless local area network
MPEG	Moving picture experts group		

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj završni rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog rada pod naslovom **Analiza programskih alata za logičku provjeru mrežnih protokola**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student:

U Zagrebu, 4. 9. 2017. Dino Kos

(potpis)