Analiza mrežnog prometa primjenom programske podrške Wireshark

Grgurić, Tomislav

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Tomislav Grgurić

ANALIZA MREŽNOG PROMETA PRIMJENOM PROGRAMSKE PODRŠKE WIRESHARK

ZAVRŠNI RAD

Zagreb, veljača 2016.

Sveučilište u Zagrebu
FAKULTET PROMETNIH ZNANOSTI
Vukelićeva 4, 10000 Zagreb
PREDDIPLOMSKI STUDIJ

Preddiplomski studij: Promet
Zavod: za informacijsko komuniakcijski promet
Predmet: Računalne mreže

ZADATAK ZAVRŠNOG RADA

Pristupnik: Tomislav Grgurić
Matični broj: 0135218771
Smjer: Informacijsko komunikacijski promet

ZADATAK:

ANALIZA MREŽNOG PROMETA PRIMJENOM PROGRAMSKE PODRŠKE WIRESHARK

ENGLESKI NAZIV ZADATKA:

WIRESHARK NETWORK TRAFFIC ANALYZER

Opis zadatka:

Opisati protiokole u TCP/IP referentnom modelu. Analizirati značajke mrežnog prometa primjenom programske podrške Wireshark.

Zadatak uručen pristupniku:
24. ožujak 2015.

Nadzorni nastavnik:

Predsjednik povjerenstva za završni ispit:

Djelovođa:

Sveučilište u Zagrebu

Fakultet prometnih znanosti

ZAVRŠNI RAD

ANALIZA MREŽNOG PROMETA PRIMJENOM PROGRAMSKE PODRŠKE WIRESHARK

Analysis Of Network Traffic Using The Software Wireshark

Mentor: Prof. dr. sc. Zvonko Kavran

Student: Tomislav Grgurić, 0135218771

Zagreb, veljača 2016.

SAŽETAK

Wireshark je programski alat za analizu mrežnog prometa prvotno nazvan *Ethereal* koji je nastao 1997. godine i od onda se razvija i nadograđuje. U ovom završnom radu izlaže se primjena i mogućnosti *Wireshark* alata u funkciji praćenja i analize mrežnog prometa. Praćenje i analiza mrežnog prometa predstavlja hvatanje i rad s uhvaćenim mrežnim paketima kao i uvoz i izvoz paketa. *Wireshark* je moguće koristiti za administraciju i povećanje sigurnosti računalnih mreža. U radu je osim osnovnih značajki ovog programskog alata dana i usporedba s drugim programskim alatima kao što su *tcpdump* i *dSniff*.

Ključne riječi: *Wireshark*; analiza mrežnog prometa; programski alat; računalne mreže

SUMMARY

Wireshark is a software tool for analyzing network traffic originally called Ethernal Which was created in 1997 and since then develops and builds. In the final work presents the application and features of Wireshark tool in the function of monitoring and analyzing network traffic. Monitoring and analysis of network traffic is captured network packets as well as import and export packages. Wireshark can be used to administer and increase the security of computer networks. In this paper, in addition to the basic features of this software tool on a comparison with other software tools such as tcpdump and Dsniff.

Kexwords: Wireshark; analysis network traffic; computer network

Sadržaj:

1.UVOD

Računalna mreža je skup dva ili više međusobno povezanih računala koja mogu dijeliti resurse. U širem smislu računalna mreža sadrži i ostale čvorove kao što su prospojnik (eng. *switch*) ili usmjernik (eng. *router*) koji koriste komunikacijske protokole u međusobnoj komunikaciji. Komunikacijski protokol je skup jednoznačno određenih pravila koja se moraju poštivati prilikom razmjene informacija. Skup komunikacijskih protokola koji omogućavaju komunikaciju između dva entiteta mreže naziva se komunikacijska arhitektura.

Wireshark, izvorno nazvan *Ethereal* je trenutno najsofisticiraniji besplatni alat koji se koristi za praćenje podataka, analizu mrežnog prometa, rješavanje mrežnih problema, razvoj mrežnih protokola i edukaciju. *Wireshark* je *''cross – platform*'' mrežni alat što znači da može raditi na više platforma kao što su: Microsoft Windows, Linux, Mac OS X i *Solaris*. Naslov završnog rada je: **Analiza mrežnog prometa primjenom programske podrške *Wireshark*.** Rad je podijeljen u šest cjelina:

1. Uvod
2. Povijesni razvoj alata *Wireshark*
3. Način rada i mogućnosti *Wireshark* alata
4. Primjeri korištenja *Wireshark* alata
5. Prednosti *Wireshark-a* u odnosu na druge alate
6. Zaključak

U drugom poglavlju je opisan povijesni razvoj programskog alata od njegovog početka do izlaska alata u inačici 1.0

U trećem poglavlju su objašnjeni TCP/IP mrežni slojevi, njihovi protokoli i vrste računalnih mreža s kojih *Wireshark* može hvatati pakete te grafičko sučelje.

Četvrto poglavlje obuhvaća primjenu *Wireshark* alata: hvatanje, uvoz, izvoz i rad s uhvaćenim paketima.

U petom poglavlju je provedena kratka usporedba *Wireshark* alata u odnosu na slične mu alate te njegove prednosti.

2. POVIJESNI RAZVOJ ALATA WIRESHARK

Gerald Combs je 1997. godine zbog potrebe za alatom za praćenje prometa na mreži i želje da nauči više o upravljanju i administriranju mreže počeo pisati program zvan *Ethereal,* preteču današnjeg *Wiresharka.* Alatom *Ethereal* htio je riješiti oba gore navedena problema. *Ethereal* je inicijalno pušten na tržište, nakon nekoliko stanki u razvoju, u srpnju 1998. godine u inačici 0.2.0. Vremenom se *Ethereal* nadogradio, ispravljene su postojeće greške i polako se počeo nazirati uspjeh projekta. Nedugo nakon toga, sistemski inženjer Gilbert Ramirez je uočio potencijal *Ethereala* i postao prvi suradnik projekta u kojeg je implementirao nekoliko radnji.[1]

U Listopadu 1998. godine, Guy Harris iz tvrtke *Network Appliance* pokušao je pronaći bolji alat za administriranje mreže od dotad korištenog alata *tcpview,* te je također počeo razvijati zakrpe i poboljšanja za *Ethereal*. Krajem 1998. godine i Richard Sharpe, stručnjak s područja TCP/IP protokola, je uočio potencijal ovog alata te počeo pisati zakrpe i unaprjeđenja za protokole koji su mu bili potrebni. Do danas se lista ljudi koji su pridonijeli razvitku alata znatno povećala. Većina tih ljudi je je započela s novim protokolima koji su im bili potrebni, a koje *Ethereal*, ili kasnije *Wireshark,* nisu još podržavali. To je dovelo do velikog broja protokola koje *Wireskark* podržava danas.[1]

Godine 2006. projekt se restrukturirao pod današnjim imenom *Wireshark*. U proljeće 2008. godine, nakon deset godina razvoja, *Wireshark* je napokon izašao u inačici 1.0. Ta inačica je bila prva potpuna inačica koja je izašla na tržište, ali je isto tako bila i inačica s minimalnim značajkama. Dakle, predstavljala je osno

vnu inačicu s mogućnošću nadogradnje. Inačica 1.0. izašla je istovremeno s održavanjem prve *Wireshark* konferencije za programere i korisnike nazvale *SharkFest.* Magazin *eWEEK* (*The Enterprise Newsweekly*) tjedni poslovni informatički magazin, je proglasio *Wireshark* „najutjecajnijom (*open source)* otvoreni izvor, aplikacijom svih vremena“.[1]

Mogućnosti alata *Wireshark* su različite, a najbitnije, koje i njegov proizvođač ističe, su:

- Hvatanje podatkovnih paketa s mrežnog sučelja
- Prikazivanje paketa s vrlo detaljnim informacijama o mrežnom protokolu
- Otvaranje i spremanje paketa
- Uvoz i izvoz podataka u druge slične programe
- Pretraga i filtriranje paketa po raznolikim kriterijima

Gotovo svi dijelovi *Wiresharka* su implementirani u programskom jeziku C. Osim uobičajenog razvoja programa u jeziku C, neki programski alati, kasnije dodavani u *Wireshark*, napisani su u drugim programskim jezicima. Neki od ti alata, odnosno programskih jezika su:

- *Perl* – služi za izradu dokumentacije
- *Pyton* i *Sed* – mogu poslužiti za generiranje nekih protokola, funkcija ili biblioteka
- *Flex* i *Bison* – mogu se koristiti pri izradi biblioteka.

3. NAČINI RADA I MOGUĆNOSTI ALATA WIRESHARK

Programska podrška *Wireshark* podržava razne protokole kao što su TCP/IP internet protokoli/protokoli mobilne telefonije (*transmission control protocol/Internet protocol*), VOIP prijenos govora Internetom (*Voice Over* IP), protokole kao i WAP protokoli za bežičnu komunikaciju (*Wireless Application Protocol*). *Wireshark* može očitati pakete s više vrsta mreža.[2]

3.1 INTERNET PROTOKOLI

Internet protokol predstavlja dogovor između dvije jedinice o načinu međusobne komunikacije - skup pravila o formatu i značenju paketa ili poruka koje se razmjenjuju između procesa istog sloja.[3]

Najraširenији i najkorišteniji referentni model interneta je TCP/IP model, sastoji se od četiri sloja, svaki sloj ima svoje protokole.[2]

Slojevi TCP/IP referentnog modela:

1. Sloj podatkovne veze
2. Mrežni sloj
3. Transportni sloj
4. Aplikacijski sloj

Zadatak sloja veze podataka je dostava datagrama iz jednog čvora mreže do susjednog čvora. Protokoli koje pri tome koristi su:

- Protokoli s čekanjem (*stop and wait*) – protokol kod kojeg pošiljatelj pošalje jedan okvir i čeka na potvrdu prije nego počne slati sljedeće okvire.
- Jednosmjerni protokol bez ograničenja (*unrestricted simplex protocol*) – omogućuje slanje podataka samo u jednom smjeru, komunikacijski kanal mora bit bez smetnji, primalac može obraditi sve podatke beskonačnom brzinom. Jedini događaj je dolazak okvira.

- Protokoli s prozorom (*Sliding window protocol*) – šalje određeni broj okvira bez čekanja potvrde, potvrda zadnjeg okvira znači i potvrda svih prethodnih okvira.
- Protokoli s vračanjem (*go back n*) – u slučaju izgubljenog ili oštećenog okvira potrebno je poslati cijeli prozor okvira.

Uloga mrežnog sloja je dostaviti pakete od izvorišnog do odredišnog čvora preko niza čvorova ili izravno, pri čemu koristi ne spojnu datagramsku uslugu. Protokoli mrežnog sloja su:

- IP (*Internet protocol*) – neovisan o nižim protokolima, nema mehanizam kontrole toka, nema garancije očuvanja redosljeda datagrama. Prihvaća podatke od višeg sloja, smješta ih u podatkovno polje IP datagrama i predaje datagram sloju podatkovne veze. Definira provedbu fragmentacije. IPv4 adresa je globalni identifikator svakog mrežnog sučelja, veličine je 32 bita.
- ICMP (*Internet Control Message Protocol*) – protokol koji „upotpunjuje“ IP protokol na način da otkriva i javlja pogreške nastale pri prijenosu.
- ARP (*Address Resolution Protocol*) – određuje adresu sloja veze podataka za poznate IP adrese
- RARP (*Reverse Address Resolution Protocol*) – određuje IP adrese kada je Mac adresa poznata.

Transportni sloj omogućava logičku komunikaciju između procesa (aplikacija), razdvaja poruke u segmente i prosljeđuje ih mrežnom sloju. Protokoli transportnog sloja su:

- UDP (*User Datagram Protocol*) – ne uspostavlja konekciju, ne vrši kontrolu toka, jedina funkcija mu je multipleksiranje, demultipleksiranje i vrlo ograničena kontrola grešaka. Koristi se kada je bitno da se podaci što prije pošalju na odredište.
- TCP (*Transmission Control Protocol*) – uspostavlja se konekcija prije slanja podataka, vrši kontrolu pogrešaka i kontrolu toka. U slučaju gubitka okvira ili potvrde okvir se ponovno šalje, svaki okvir je numeriran kako bi mogli razlikovat duplikat od originala u slučaju da se izgubila potvrda o primitku okvira.

Aplikacijski sloj je najbliži krajnjem korisniku, dostavlja mrežne servise aplikacijama krajnjeg korisnika. Protokoli aplikacijskog sloja su:

- HTTP (*Hypertext Transfer Protocol*) – protokol za komunikaciju između poslužitelja (servera) i klijenta, koristi TCP protokol mrežnog sloja. Konekcija i komunikacija sa serverom se završava odmah nakon isporučenog paketa traženih podataka.
- FTP (*File Transfer Protocol*) – omogućava dvosmjerni prijenos podataka, za razliku od HTTP protokola koristi dvije TCP konekcije, kontrolnu i konekciju za podatke.
- SMTP (*Simple Mail Transfer Protocol*) – koristi se za prijenos elektroničke pošte, sve poruke moraju biti u sedmobitnom ASCII formatu.

3.2 PROTOKOLI ZA PRIJENOS ZVUČNE KOMUNIKACIJE PUTEM INTERNETA

Tehnologija za prijenos zvučne komunikacije ili *VoIP* postala je popularna razvojem širokopojasnog interneta. Prilikom uspostave poziva, koristi se paketski prijenos zvuka. Omogućava besplatno telefoniranje. Koristi razne protokole kao što su:

- SIP (*Sesion Initiation Protocol*) – Određuje trenutnu IP adresu pozvane osobe, upravlja pozivom. Omogućava dodavanje novih stream-ova i promjenu kodiranja za vrijeme poziva.
- H.323 – alternativa SIP-u, sveobuhvatan standard koji propisuje kontrolni protokol H.245, signalni kanal Q.931 i protokol RAS (*Remote access Service*) za registraciju kod čuvara prolaza.

3.3 VRSTE MREŽA S KOJIH WIRESHARK MOŽE OČITATI PAKETE

Računalne mreže je moguće podijeliti na više načina. Možemo ih podijeliti prema tehnologiji prijenosa, području koje pokrivaju, topologiji i vrsti protokola koje koriste. Mogućnost hvatanja paketa pomoću *Wireshark* programskog alata s određenih mreža ovisi o protokolima koje te mreže koriste za prijenos podataka.

Wireshark alat podržava više vrsta mreža, najpoznatije su:

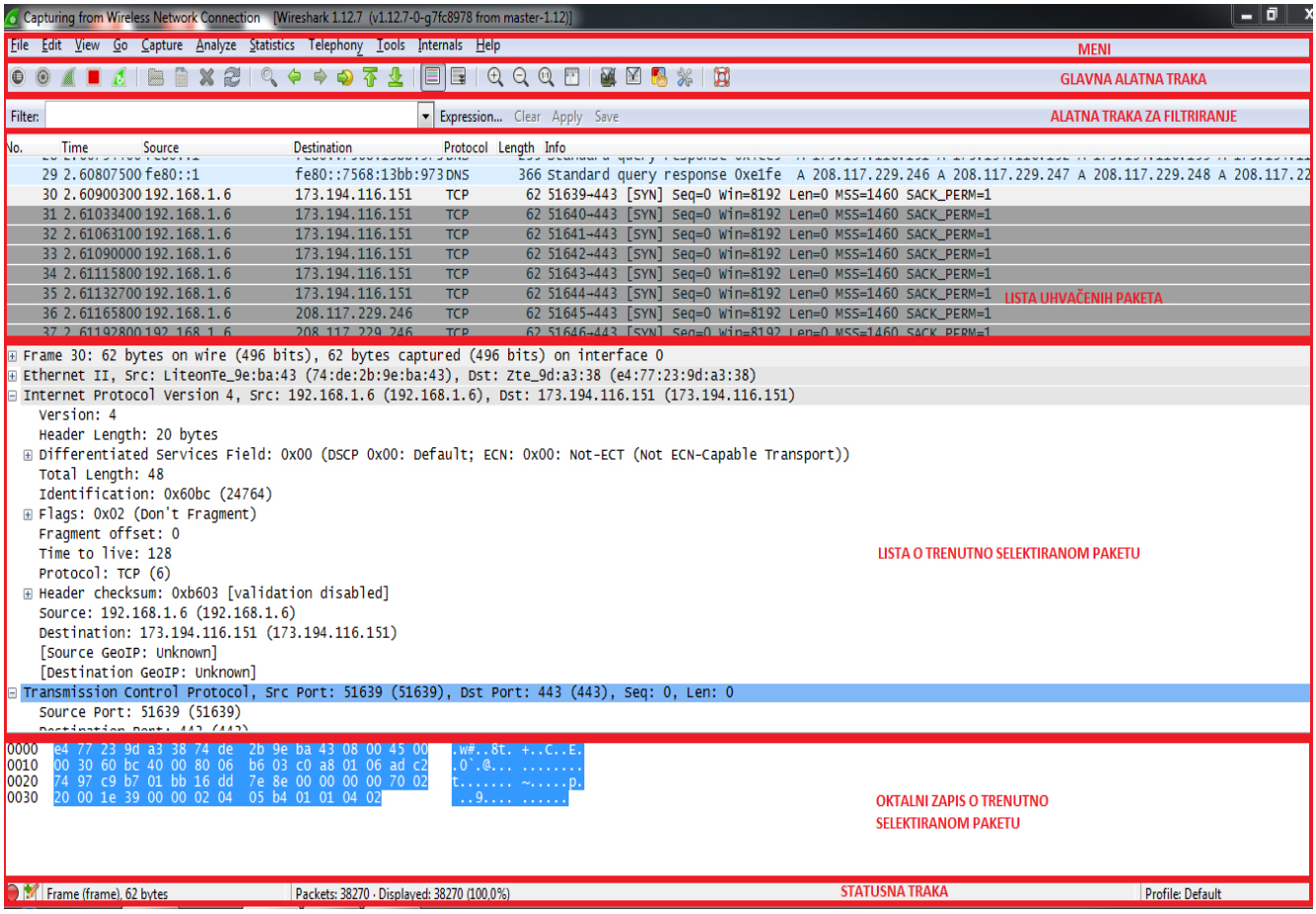
- *Ethernet* – prva široko korištena tehnologija u lokalnim mrežama (*Local Area Network - LAN*) mrežama, brzine prijenosa od 10MB do 10 GB. Ima mogućnost slanja prema jednom (*Unicast*) ili prema više (*Multicast/Broadcast*) prijamnika.
- IEEE 802.11 – standardi za bežičnu komunikaciju računala, koristi frekvencijske pojaseve od 2.4, 3.6, i 5 GHz.

- Protokol za izravno povezivanje dvaju čvorova (*Point-to-Point Protocol*-PPP)- koristi se za izravno povezivanje dvaju čvorova. Omogućava povezivanje dvaju računala posebnom radio ili satelitskom vezom te telefonskim ili optičkim kabelom.

3.4 GRAFIČKO SUČELJE

Izgled prozora analize uhvaćenih paketa prikazan je na slici 2. Grafičko sučelje se sastoji od:

- Meni- služi za pokretanje akcija
- Glavna alatna traka
- Alatna traka za filtriranje
- Lista uhvaćenih paketa
- Lista o trenutno selektiranom paketu
- Oktalni zapis trenutno selektiranog paketa
- Statusna traka



Slika 1. Prikaz prozora analize uhvaćenih paketa

Opcije koje omogućuju pojedini dijelovi grafičkog sučelja:

Meni:

• *File* – pruža mogućnosti otvaranja i spajanja različitih datoteka te spremanja ispisa i izvoženja kompletnih ili dijelova uhvaćenih paketa.

• *Edit* – pruža mogućnosti traženja paketa, njihovog referenciranja i vremenskog označavanja. Omogućuje i postavljanje vlastitih referenci u programu

• *View* – omogućuje kontrolu prikaza uhvaćenih paketa

• *Go* – pruža opciju pozicioniranja na određeni paket

• *Capture* – podešava filtriranje paketa koji se hvataju te omogućuje pokretanje i zaustavljanje hvatanja paketa

• *Analyze* – pruža mogućnosti prikazanih filtara, omogućavanje analize protokola te konfiguriranje korisničkih dekodiranja uhvaćenih paketa

• *Statistic* – omogućuje prikaz raznih statistika

• *Telephony* – prikazuje statistike za telefoniju

• *Tools* – omogućuje korištenje Lua programskog jezika

• *Internals* – pruža informacije o unutrašnjim funkcioniranjima samog Wireshark alata

• *Help* – pruža korisniku pomoć pri korištenju alata

Alatna traka za filtriranje:

• *Filter* - omogućuje unos protokola na temelju kojeg želimo filtrirati pakete

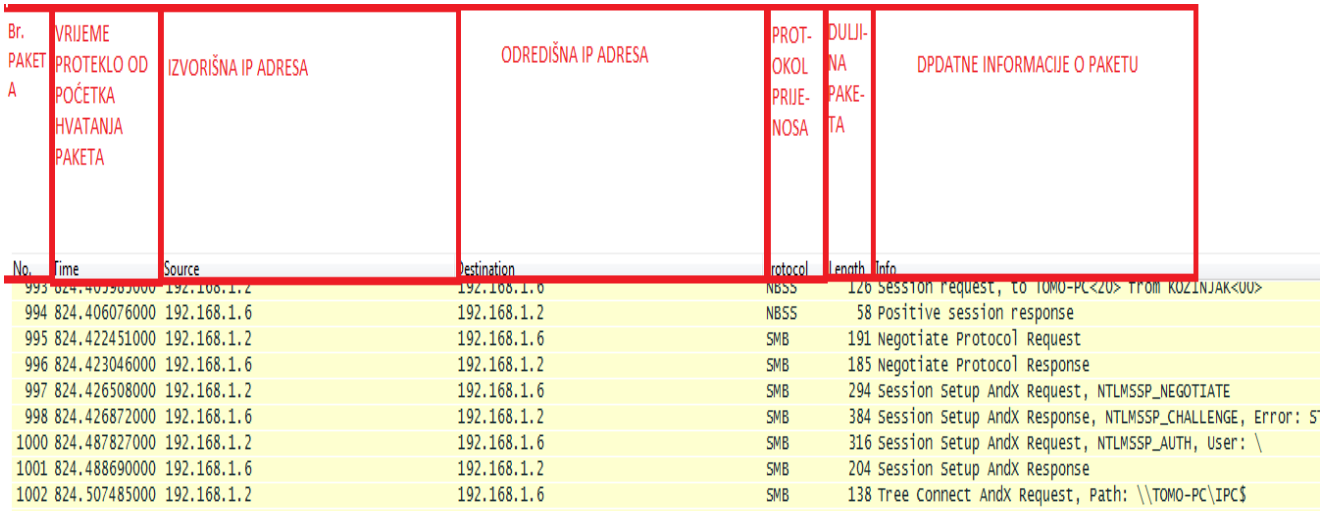
• *Expression* – nudi popis protokola na temelju kojih želimo filtrirati podatke

• *Clear* – resetira trenutni prikaz filtra

• *Apply* – primjenjuje trenutnu vrijednost filtra

• *Save* – sprema pakete koji su prošli kroz filtar

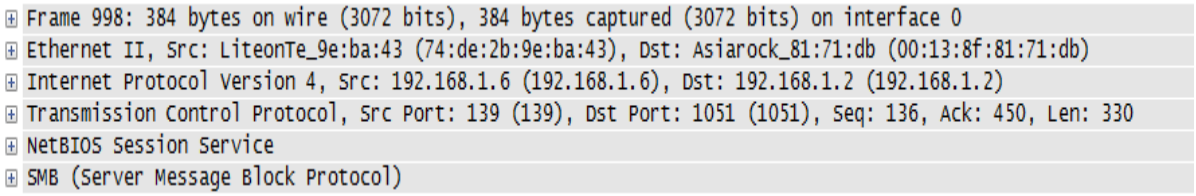
Lista uhvaćenih paketa prikazuje uhvaćene pakete i osnovne informacije kao što je prikazano na slici 3.



Slika 2. Lista uhvaćenih paketa

Lista detalja o selektiranom paketu

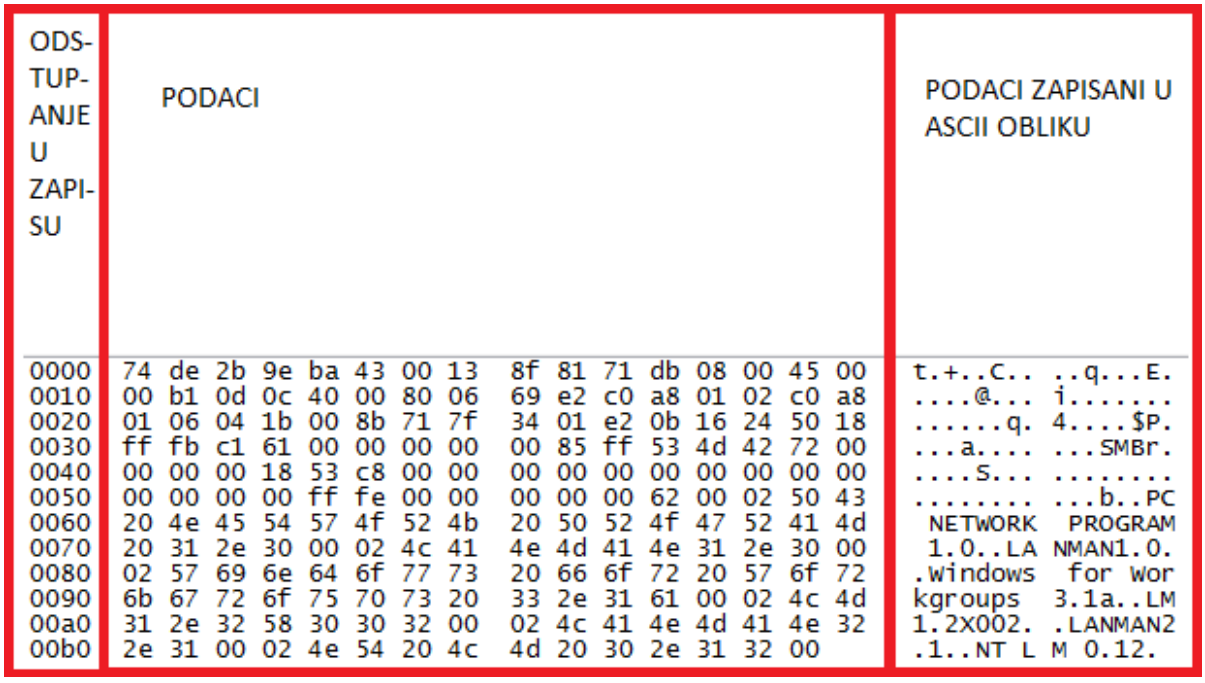
Na listi detalja o selektiranom polju nalazi se podaci o okviru, vrsti mreže, verziji IP protokola, vrsti transportnog protokola, spojnoj ili ne spojnoj usluzi i protokolu aplikacijskog sloja kao što je prikazano na slici 4.



Slika 3. Lista detalja o selektiranom paketu

Oktalni zapis selektiranog paketa

Na oktalnom zapisu paketa se nalaze podaci o odstupanju podataka u zapisu i podaci zapisani u ASCII obliku kao što je prikazano na slici 5.



ODS-TUP-ANJE U ZAPI-SU	PODACI	PODACI ZAPISANI U ASCII OBLIKU
0000	74 de 2b 9e ba 43 00 13 8f 81 71 db 08 00 45 00	t.+..C.. ..q...E.
0010	00 b1 0d 0c 40 00 80 06 69 e2 c0 a8 01 02 c0 a8	....@... i.....
0020	01 06 04 1b 00 8b 71 7f 34 01 e2 0b 16 24 50 18	......q. 4....$P.
0030	ff fb c1 61 00 00 00 00 00 85 ff 53 4d 42 72 00	...a.... ...SMBr.
0040	00 00 00 18 53 c8 00 00 00 00 00 00 00 00 00 00	....S... ....
0050	00 00 00 00 ff fe 00 00 00 00 00 62 00 02 50 43	....b..PC
0060	20 4e 45 54 57 4f 52 4b 20 50 52 4f 47 52 41 4d	NETWORK PROGRAM
0070	20 31 2e 30 00 02 4c 41 4e 4d 41 4e 31 2e 30 00	1.0..LA NMAN1.0.
0080	02 57 69 6e 64 6f 77 73 20 66 6f 72 20 57 6f 72	.Windows for Wor
0090	6b 67 72 6f 75 70 73 20 33 2e 31 61 00 02 4c 4d	kgroups 3.1a..LM
00a0	31 2e 32 58 30 30 32 00 02 4c 41 4e 4d 41 4e 32	1.2X002. .LANMAN2
00b0	2e 31 00 02 4e 54 20 4c 4d 20 30 2e 31 32 00	.1..NT L M 0.12.

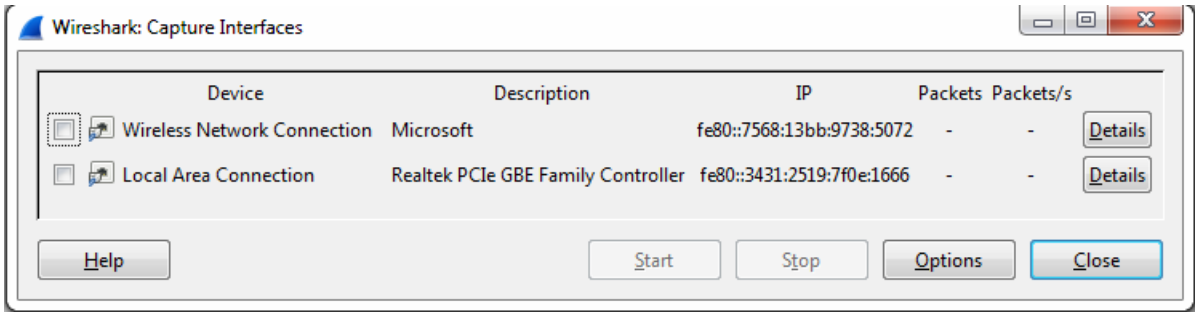
Slika 4. Lista o oktalnom zapisu selektiranog paketa

4. PRIMJERI KORIŠTENJA WIRESHARK ALATA

Programska podrška *Wireshark* se najčešće koristi za hvatanje, filtriranje, uvoz i izvoz paketa. Omogućuje prekid hvatanja paketa, reduciranje količine uhvaćenih paketa, hvatanje s različitih vrsta mreža i filtriranje paketa. *Wireshark* u odnosu na ostale alate ima grafičko sučelje što omogućava jednostavnije rukovanje alatom

4.1 HVATANJE MREŽNIH PAKETA

Hvatanje mrežnih paketa jedno je od glavnih obilježja *Wireshark* alata. Nakon pokretanja alata na glavnoj alatnoj traci odaberemo opciju „*Capture*“, zatim „*Interfaces*…“ nakon toga nam se pojavi prozor s ponuđenim opcijama kao što je prikazano na slici 6.



Slika 5. Sučelje za hvatanje paketa

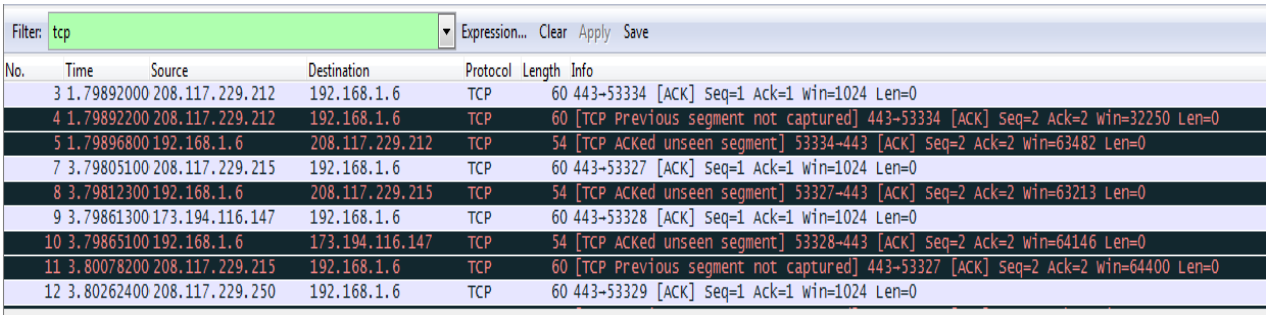
Opcijom „Start“ se pokreće hvatanje paketa, prije nego bude omogućeno hvatanje paketa potrebno je odabrati uređaj s kojeg želimo hvatati pakete, možemo izabrati samo jedan i više njih.

4.2 FILTRIRANJE MREŽNIH PAKETA

Nakon što je pokrenuto hvatanje paketa, otvara se novi prozor u kojem se nalaze uhvaćeni paketi. Upisivanjem imena protokola ili odabirom protokola na alatnoj traci za filtriranje i odabirom opcije „*apply*“ izvršava se filtriranje paketa. Filtriranje paketa je moguće provesti na temelju IP adrese, veličine paketa, postojanja podataka u paketu, sličnosti među paketima kao i mnoge druge selekcije.

Osnovne mogućnosti postavljanja primitiva su:

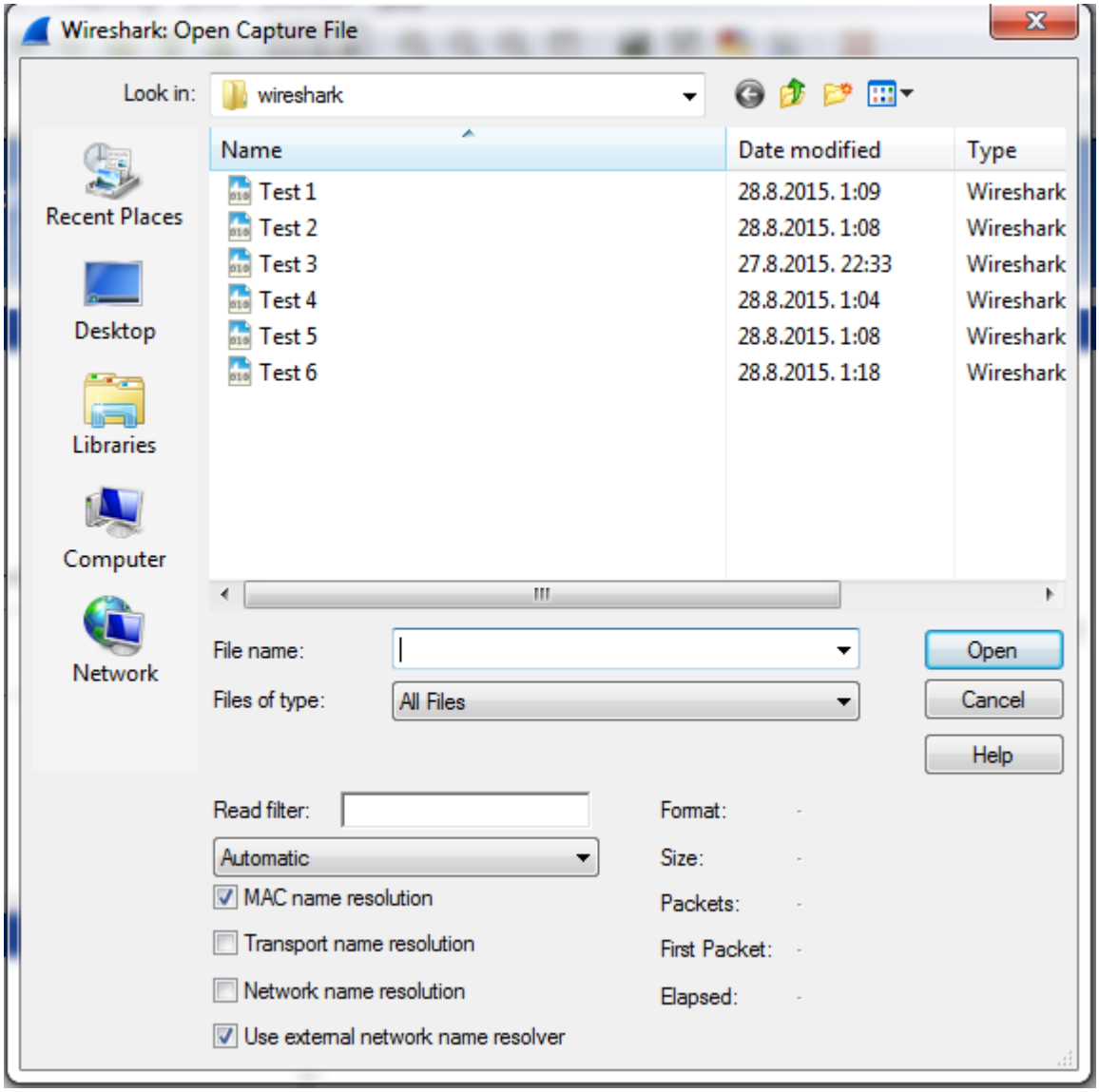
- [*src/dst*] *host* <*host*> ; Ovim zapisom odabire se filtriranje po IP adresi. Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana IP adresa odredišna odnosno izvorišna.
- *ethr[src/dst] host* <*ehost*> ; Zapis omogućuje filtriranje po *eternet* adresi. Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana adresa odredišna odnosno izvorišna.
- *Gateway host* <*host*> ; Zapis omogućuje filtriranje paketa koji su koristili postavljeni *host* kao *gateway*.
- [*src/dst*] *net* <*net*> [{*mask*<*mask*>}\{*len*<*len*>}]; Zapis omogućuje filtriranje po mrežnim adresama odnosno po *NetId-u.* Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana adresa odredišna odnosno izvorišna.
- *[tcp/udp] [src/dst] port*<*port*>; Zapis omogućuje filtriranje po protokolu ovisno o tome je li protokol TCP ili UDP. Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana adresa odredišna odnosno izvorišna.
- *less/greater* <*length*>; Zapis omogućuje filtriranje paketa čija je veličina veća ili jednaka zadatoj odnosno manja ili jednaka zadatoj
- *ip/ether* proto <*protocol*>; Zapis omogućuje filtriranje po protokolima mrežnog i *ethernet* sloja.
- *ip/ether brodcast/multicast*; Zapis omogućuje filtriranje ovisno o tome da li je adresa razašiljanja paketa više odredišna ili jedno odredišna. [2]



Slika 6. Prikaz filtriranih paketa na temelju TCP protokola

4.3 UVOZ I IZVOZ PODATAKA

Wireshark ima mogućnost čitanja paketa spremljenih u datoteke. Čitanje je moguće izvesti pomoću opcije „File“ koja se nalazi na glavnoj alatnoj traci, nakon odabira opcije „File“ odabiremo opciju „Open“, otvara se prozor u kojem se nalaze spremljene datoteke kao što je prikazano na slici 8.



Slika 7. Prikaz prozora u kojem se nalaze spremljene datoteke

Wireshark podržava više formata za izvoz podataka. Najjednostavniji i najčešće korišten način izvoza podataka je u ASCII tekstualnom formatu. Takav način izvoza podataka u *Wiresharku* je moguće napraviti odabirom opcije „*File/Export*“. Izvoz podatak moguć je i u drugim formatima oni su:

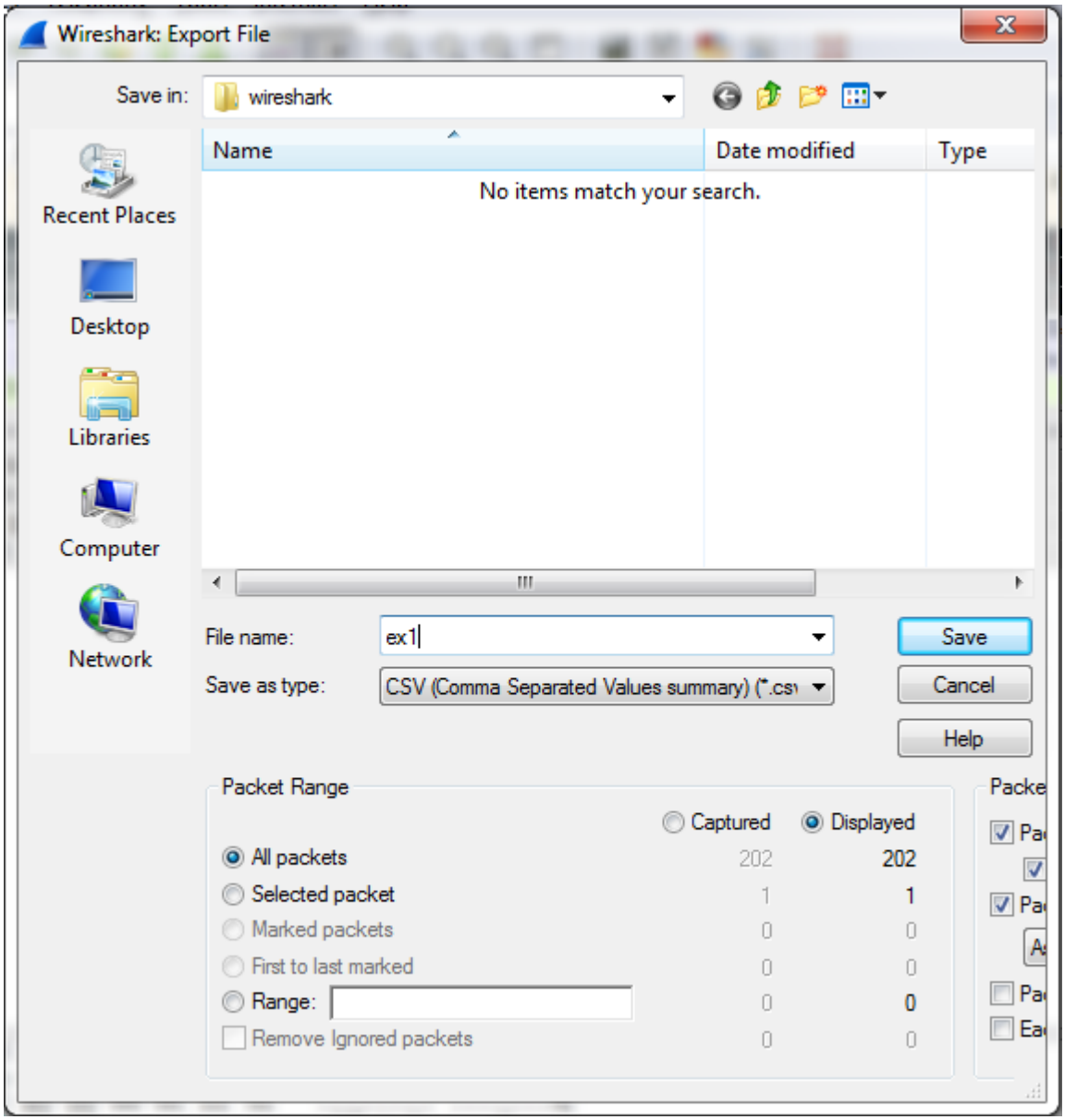
• PostScript

• CSV (*Comma Separated Values*)

• polja programskog jezika C

• PSLM

• PDML[2]



Slika 8. Prikaz izvoza podataka u CSV formatu

4.4 RAD S UHVAČENIM PAKETIMA

Nakon što su paketi uhvaćeni ili nakon što je datoteka s informacijama o prethodno uhvaćenim paketima učitana popis paketa vidljiv je u listi paketa. Fokusiranjem na neki od paketa iz liste biti će prikazane detaljne informacije o tome paketu. [2] Informacije o paketima možemo podijeliti u 2 skupine kao što je prikazano na slici 9., a to su: lista uhvaćenih paketa i analiza sadržaja paketa.

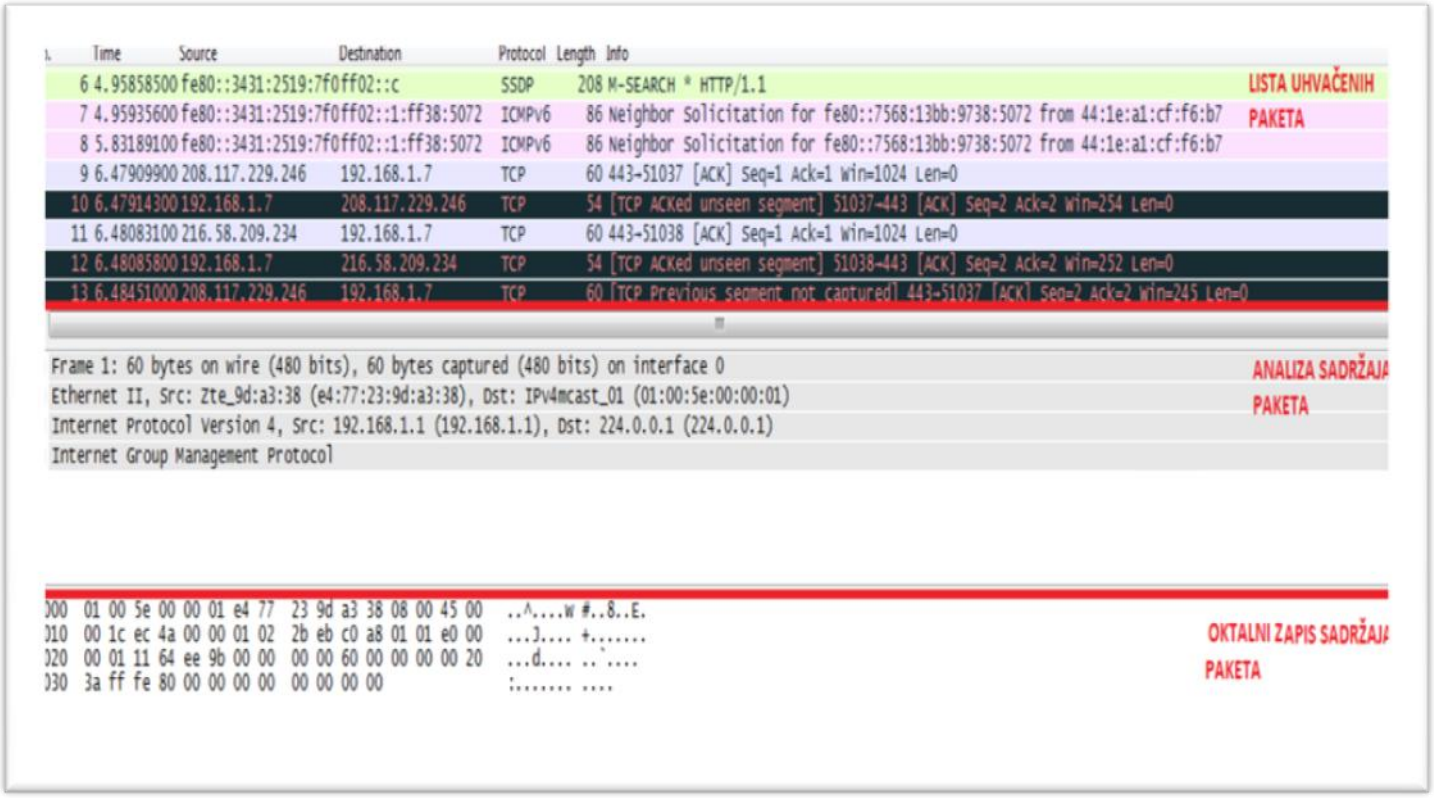
Informacije o paketu koje možemo iščitati iz liste uhvaćenih paketa su sljedeće:

- *No.* : redni broj uhvaćenog paketa,
- *Time:* vrijeme proteklo od početka hvatanja paketa, vrijeme je izraženo u sekundama,
- *Source:* prikaz adrese pošiljatelja,
- *Destination:* prikaz adrese primatelja,
- *Protocol:* Vrsta protokola koji se koristi za prijenos paketa od pošiljatelja do primatelja,
- *Lenght:* duljjina paketa, izražena u bajtima,
- *Info:* informacije o sadržaju paketa

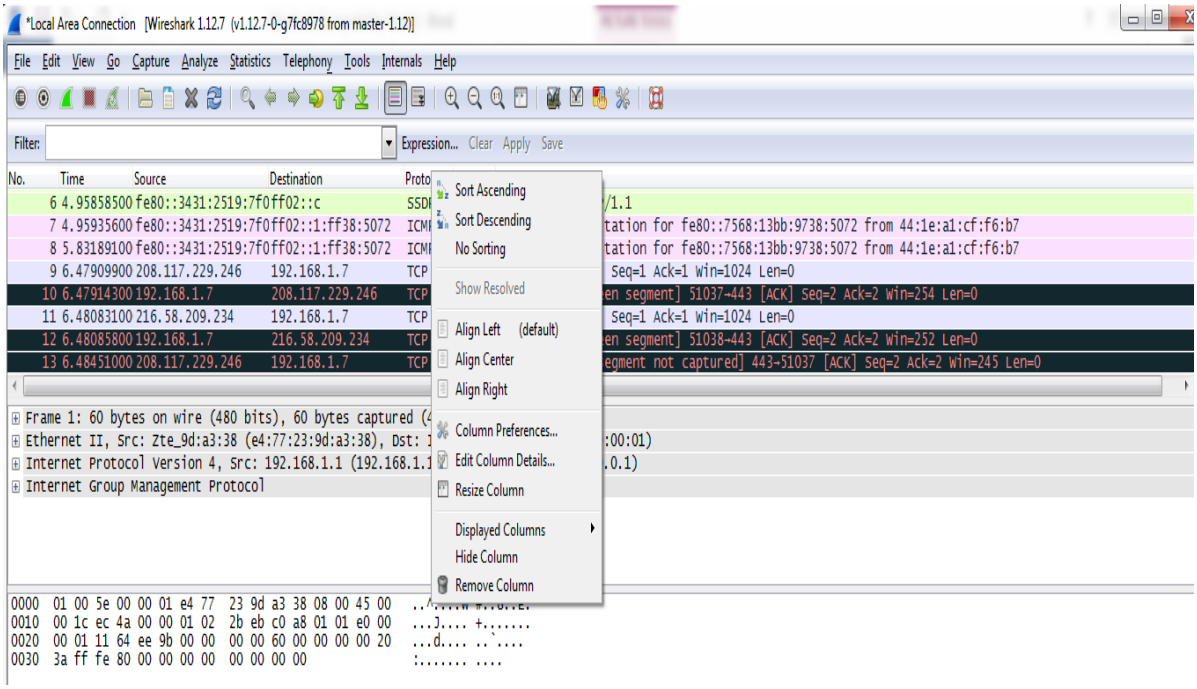
Analiza sadržaja paketa sadrži sljedeće informacije:

- *Frame:* sadrži informacije o duljini paketa, vrsti sučelja, vrsti enkapsulacije paketa, vrijeme primitka paketa i vremensku zonu u kojoj se nalazi primatelj paketa, dužinu paketa, te dužinu paketa koja je uhvaćena prilikom hvatanja paketa.
- *Ethernet II:* sadrži informacije o pošiljatelju i primatelju te verziju Internet protokola.
- *Internet protocol:* nudi informacije o verziji protokola koji se koristi, izvorišnu i odredišnu *IP* adresu, *checksum,* i informacije o fragmentaciji paketa.

- *Protokoli transportnog sloja:* Sadrži informacije o vrsti protokola, broj izvorišnog i odredišnog protokola, broj potvrde o prispjeću paketa, duljina zaglavlja izražena u bajtima, indeks propusnosti paketa kroz mrežu.



Slika 9: Prikaz uhvaćenih paketa i informacije o paketima



Slika 10. Opcije ponuđene desnim klikom na ime stupca liste uhvaćenih elemenata

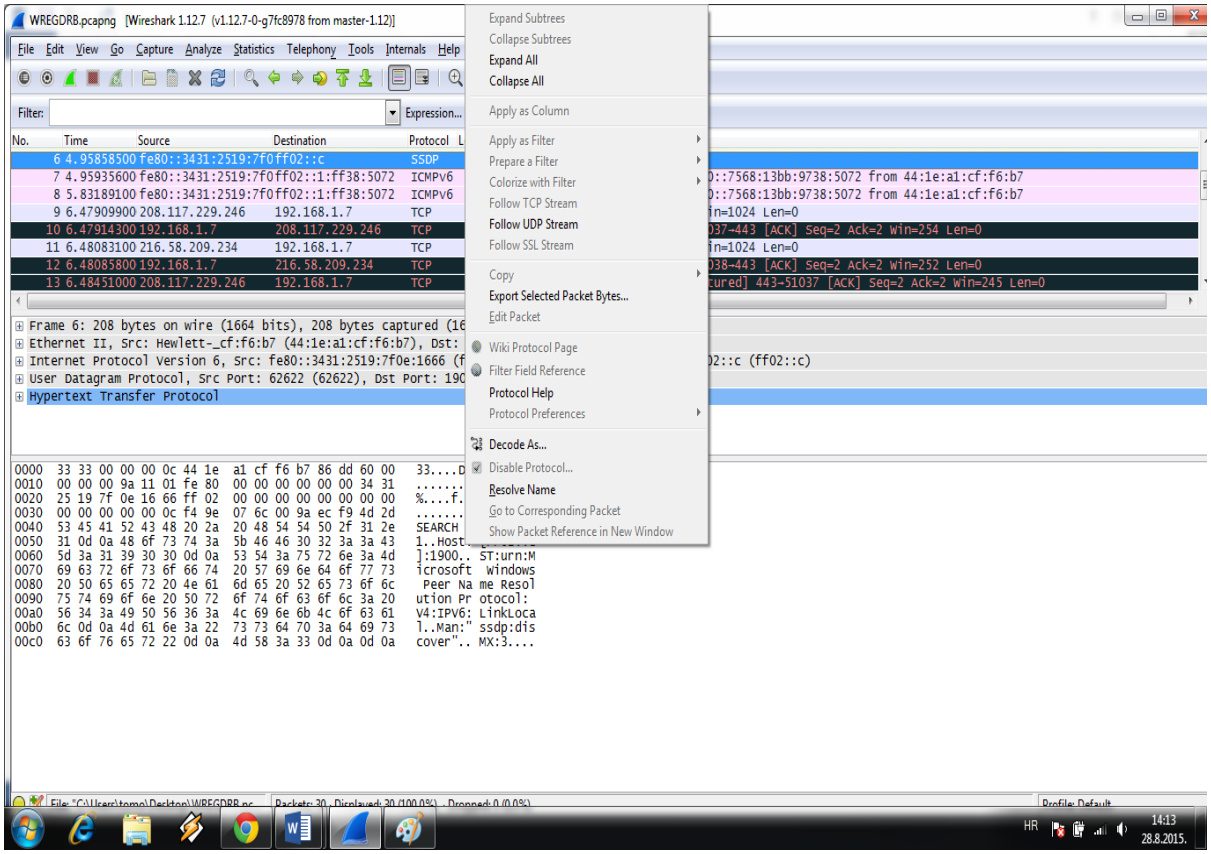
Funkcionalnosti ponuđenog izbornika objašnjene su u tablici 1.

Stavka	**Opis**
Sort Ascending	Omogućuje uzlazno sortiranje elemenata u listi na osnovu vrijednosti odabranog stupca
Sort Descending	Omogućuje silazno sortiranje elemenata u listi na osnovu vrijednosti odabranog stupca
No Sort	Uklanja sortiranje na osnovu odabranog stupca.
Align Left	Lijevo poravnava sadržaj stupca
Align Center	Centralno poravnava sadržaj stupca
Align Right	Desno poravnava sadržaj stupca
Column Preferences…	Otvara prozor za postavljanje korisničkih postavki
Resize Column	Prilagođava veličinu stupca da odgovara njegovom sadržaju
Rename Column Title	Omogućuje preimenovanje stupca

Stavka	Opis
Displayed Column	Prikazuje listu konfiguriranih stupaca
Hide Column	Omogućuje skrivanje odabranog stupca
Remove Column	Omogućuje uklanjanje stupca iz liste uhvaćenih paketa.

Tablica 1. Popis funkcionalnosti izbornika za rad s stupcima u listi uhvaćenih paketa, [2]

Prikaz opcija ponuđenih desnim klikom na element liste uhvaćenih paketa prikazan je na slici



Slika 11. Opcije uhvaćenog elementa

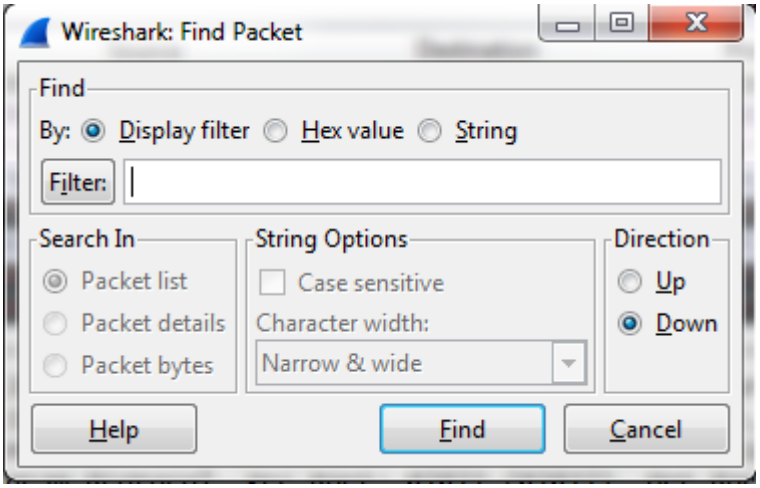
Funkcionalnosti ponuđenog izbornika objašnjene su u tablici 2.

Stavka	**Opis**
Expand Subtrees	Proširuje stablo informacija o odabranom paketu
Collapse Subtrees	Skriva detalje stabla informacija o odabranom paketu
Expand All	Proširi stabla informacija svih uhvaćenih paketa
Collapse All	Sakriva detalje stabla informacija svih uhvaćenih paketa
Apply as Column	Od odabranog protokola stvara novi stupac u listi uhvaćenih paketa
Apply as Filter	Primjenjuje pripremljeni prikazni filtar
Prepare a Filter	Omogućuje pripremu filtra na osnovu trenutno odabranog elementa
Colorize with Filter	Omogućuje bojanje odabrane stavke ovisno o trenutno odabranom prikaznom filtru.

Stavka	Opis
Follow TCP Stream	Omogućuje pregled svih podataka na TPC toku između dva mrežna čvora
Follow UDP Stream	Omogućuje pregled svih podataka na UDP toku između dva mrežna čvora
Follow SSL Stream	Omogućuje pregled svih podataka na SSL toku između dva mrežna čvora
Copy/ Description	Omogućuje kopiranje informacija o trenutno odabranom polju
Copy/ Fieldname	Omogućuje kopiranje imena trenutno odabranog polja
Copy/ Value	Omogućuje kopiranje sadržaja trenutno odabranog polja
Copy/ As Filter	Priprema prikazni filtar na temelju trenutno odabrane stavke i omogućuje njegovo kopiranje.
Export Selected Packet Bytes…	Omogućuje izvoz trenutno odabrane stavke u bajtovnom prikazu.
Wiki Protocol Page	Otvara informacijsku stranicu o trenutnom odabranom protokolu.
Filter Field Reference	Otvara informacijsku strancu o filtru trenutno odabrane stavke.
Protocol Preferences…	Otvara prozor za postavljanje postavki vezanih uz protokole
Decode As…	Omogućuje postavljanje novog načina interpretacije podataka.
Disable Protocol	Onemogućuje trenutnu interpretaciju protokola tj. podatka
Resolve Name	Omogućuje identifikaciju MAC, IP ili transportne adrese trenutno odabranog paketa.
Go to Corresponding Packet	Prebacuje fokus na korespondentni paket u listi uhvaćenih paketa.

Tablica 2. Popis funkcionalnosti izbornika za rad s elementima u listi uhvaćenih paketa, [2]

Pronalaženje određenog paketa provodi se stiskom na stavku glavne alatne trake koja pokreće prozor za traženje paketa. U ovom prozoru moguće je specificirati uvijete pretraživanja. Primjer prozora dan je na slici 13.



Slika 12. Prozor za pronalaženje paketa

Prozor za pronalaženje paketa sadrži opcije :

- *Filter*: postavljanje filtra, odabir načina filtriranja
- *Search In*: postavljanje dubine pretraživanja
- *String Options*: Traženje odrađenog teksta u podacima
- *Direction*: smjer pretraživanja

5. PREDNOSTI WIRESHARK-A U ODNOSU NA DRUGE ALATE

Wireshark je alat koji spada u skupinu besplatnih mrežnih analizatora. Neki od sličnih besplatnih alata za mrežnu analizu su:

• *Capsa Free*,

• *Cain & Abel,*

• *dSniff,*

• *Ettercap*

• *Microsoft Network Monitor*

• *Ngrep*

• *snoop*

• *tcpdump* [1]

Izuzev *Wiresharka*, Najpoznatiji i najrašireniji među mrežnim analizatorima su *dSniff* i *tcpdump. Tcp dump* je alat za analizu mreže koji se koristi za praćenje problema na mreži i nadgledanje aktivnosti. Nema grafičko sučelje nego samo konzolno, pa je potrebno upisivati naredbe korištenja. *Wireshark*, s druge strane ima i grafičko sučelje te omogućuje upravljanje pomoću upisa naredbi.

Tcpdump je besplatni alat licenciran BSD (*Berkely Source Distribution*) licencom, dok je *Wireshark* licenciran već spomenutom GNU GPL licencom. I *Wireshark* i *tcpdump* podržavaju većinu operacijskih sustava (Microsoft Windows, Mac OS X, *Linux, Solaris* itd.). *Tcpdump* alat se smatra alatom "niže razine" zbog svoje kompleksnosti u odnosu na *Wireshark.* Pri korištenju *tcpdump* alata potrebno je veće znanje iz područja računalnih mreža, odnosno bolje poznavanje TCP/IP referentnog modela. Posebna inačica alata *tcpdump* za operacijski sustav *Microsoft Windows* zove se *WinDump.*

dSniff je alat po svojstvima vrlo sličan *tcpdumpu*. Informacije koje *dSniff* može pročitati su korisnička imena, lozinke, posjećene Internet stranice, sadržaj e-pošte i drugi. Nema grafičko sučelje, licenciran je od strane BSD licence i primarno napravljen za unix operacijske sustave. *Wireshark* alat podržava veliki broj protokola pa je tako moguće i vrlo jednostavno prenositi pakete uhvaćene od strane *tcpdump-a* u *Wireshark* i obrnuto.[1]

IP Sniffer je skupina alata koji se koriste za analizu mrežnog prometa. Namjenjen je za rad na svim inačicama Windows operacijskih sustava, uz određene komponenete. Mogućnosti koje pruža su brojne, od pračena propusnosti mreže, raznih statistika vezanih uz rad protokola, postavljanje različitih filtera i provjere servisa za određene protokole. Za nejgovo pravilno korištenje potrebno je imati saznanja o raznim mrežnim protokolima, uređajima, servisima i sl., kako bi korisnik bio u stanju potpuno i na ispravan način iskoristiti sve mogućnosti koje ova skupina alata pruža. U slučaju da je takvo znanje već prisutno, alati postaju prilično jednostavni za korištenje.

Microsoft Network Monitor je program za analizu mrežnog prometa koji omogućuje hvatanje, pregled i analizu mrežnog prometa. Podržava više od 300 različitih protokola. Najčešće se primjenjuje za rješavanje problema s mrežom i mrežnim aplikacijama. Osim mogućnosti hvatanja paketa na žičanim mrežama može se koristiti i za bežično hvatanje paketa.

6. ZAKLJUČAK

Nakon 10 godina razvoja *Wireshark* alat je pušten na tržište. U tom periodu mnogi stručnjaci su se uključili u razvoj alata. *Wireshark* podržava razne protokole kao što su TCP/IP protokoli, VoIP protokoli i WAP protokoli za bežičnu komunikaciju. Hvatanje paketa s određenih mreža ovisi o protokolima koje te mreže koriste za prijenos podataka. Grafičko sučelje programskog alata nam omogućava jednostavnu primjenu alata uz minimalno znanje. Analizom i praćenjem mrežnog prometa došli smo do spoznaje da nam *Wireshark* programski alat omogućuje hvatanje, filtriranje, uvoz, izvoz i rad s uhvaćenim paketima. Prilikom hvatanja paketa moramo odlučiti s kojeg sučelja na mreži želimo hvatati pakete. Hvatanje paketa jedno je od glavnih obilježja *Wireshark* alata. Pri filtriranju uhvaćenih paketa imamo mogućnost odabira filtra. Filtriranje paketa je moguće provesti na temelju IP adrese, veličine paketa, postojanja podataka u paketu. Uvozom i izvozom paketa omogućujemo promjenu formata paketa koje preuzimamo od nekog drugog programa ili predajemo pakete drugom programu. *Wireshark* podržava više formata za izvoz podataka. Nakon analize *wireshark* alata i provedene usporedbe sa sličnim alatima vidljivo je da je *Wireshark* alata najkvalitetniji besplatni alat te vrste.

LITERATURA

[1] Analiza alata Wireshark, NCERT – PUBDOC 2010 – 09 – 312, Available from: http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-09-312.pdf

[2] Wireshark, Petar Anić, Fakultet elektrotehnike i računarstva, Available from: http://os2.zemris.fer.hr/ns/malware/2014_15_ProjectMalware/Home/WiresharkPage.html

[3] prof. dr. sc Zvonko Kavran, dr. sc. Ivan Grgurević, Računalne mreže, materijali 2, Available from:

http://e-student.fpz.hr/Predmeti/R/Racunalne_mreze/Materijali/2_Predavanje.pdf

[5] A *tcpdump* Primer with Examples, Available from:

https://danielmiessler.com/study/tcpdump/

[6] Pračenje mrežnog prometa, Available from:

http://www.cis.hr/sigurosni-alati/pracenje-mreznog-prometa.html

[7] Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu, Zavod za elektroničke sustave i obradbu informacija, Laboratorij za sustave i signale. Sustavi za praćenje i vođenje procesa, Available from: http://www.fer.unizg.hr/_download/repository/LAN%5B1%5D.pdf

[8] Savjeti za korištenje Wireshark za hvatanje, filtar i pregled paketa, Available from:

http://www.yac.mx/hr/pc-tech-tips/sofware/Tips_To_Use_Wireshark_to_Capture_Filter_and_Inspect_Packets.html

[9] tehnička škola Ruđera Boškovića Zagreb, Getaldićeva 4, Dijagnostika i održavanje uređaja, Available from:

http://www.yac.mx/hr/pc-tech-tips/sofware/Tips_To_Use_Wireshark_to_Capture_Filter_and_Inspect_Packets.html

POPIS ILUSTRACIJA

PRILOZI

Prilog 1: Glavna alatna traka:

-  - popis dostupnih sučelja za praćenje prometa
-  - prikaz opcija za hvatanje paketa
-  - početak novog hvatanja paketa
-  - zaustavljanje hvatanja paketa
-  - ponovno pokretanje hvatanja paketa
-  - otvaranje spremljenih paketa
-  - spremanje uhvaćenih paketa
-  - zatvaranje datoteke s uhvaćenim paketima
-  - ponovno učitavanje uhvaćenih paketa
-  - traženje paketa
-  - pomicanje u nazad po paketima
-  - pomicanje u naprijed po paketima
-  - traženje paketa na osnovu rednog broja paketa
-  - pozicioniranje na prvi uhvaćeni paket
-  - pozicioniranje na zadnji uhvaćeni paket
-  - višebojni prikaz liste paketa
-  - automatsko pomicanje liste paketa prilikom hvatanja paketa
-  - povećanje fonta podataka o paketu
-  - smanjenje fonta podataka o paketu
-  - vraća font podataka na poćetnu velićinu
-  - prilagođava širinu stupaca koji sadrže podatke
-  - omogućuje konfiguriranje filtara za hvatanje paketa
-  - omogućuje konfiguriranje filtara za prikaz uhvaćenih paketa

-  - označava pakete određenim bojama na temelju njihovih protokola
-  - postavljanje vlastitih postavki
-  - pomoć korisniku u radu

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

METAPODACI

Naslov rada: Analiza mrežnog prometa primjenom programske podrške Wireshark

Autor: Tomislav Grgurić
Mentor: prof. Dr. Sc. Zvonko Kavran

Naslov na drugom jeziku (engleski):
Analysis of network traffic using the Wireshark Software

Povjerenstvo za obranu:

- prof. dr. sc. Dragan Peraković, predsjednik
- prof. dr. sc. Zvonko Kavran, mentor
- dr. sc. Ivan Grgurević, član
- prof. dr. sc. Slavko Šarić, zamjena

Ustanova koja je dodjelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu
Zavod: Zavod za informacijsko komunikacijski promet
Vrsta studija: sveučilišni
Naziv studijskog programa: Promet
Stupanj: preddiplomski
Akademski naziv: univ. bacc. ing. traff.
Datum obrane završnog rada: **2. veljače 2016.**

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 mrežnog prometa primjenom programske podrške Wireshark**

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

Student:

U Zagrebu, 19.1.2016 Tomislav Grgurić
(potpis)