Wireshark

Petar Afrić, 0036469979

Mentor: prof. Marin Golub
Akademska godina 2014/2015

Sadržaj

1. Uvod

Wireshark je besplatan program, otvorenog koda, za analizu mrežnog prometa, rješavanje mrežnih problema te razvoj mrežnih protokola i edukativne svrhe. Dostupan je za više različitih operacijskih sustava primjeri kojih su: GNU/Linux, OS X, BDS, Solaris i Microsoft Windows. Postoji i verzija za terminal zvana TShark. Razvijen je u programskim jezicima C i C++, a razvio ga je Wireshark tim.

Kao što je već spomenuto Wireshark je alat za analizu događanja u mreži. Kao što voltmetrom možemo mjeriti promjene napona u električnom kabelu tako wiresharkom možemo pratiti događanja u mreži. Wireshark hvata mrežne pakete te nastoji prikazati i protumačiti njihov sadržaj na najtočniji odnosno najefikasniji mogući način. Neke od mogućnosti koje wireshark pruža su:

- Hvatanje trenutnih mrežnih paketa na određenom mrežnom sučelju
- Detaljna analiza sadržaja uhvaćenih mrežnih paketa
- Pretraživanje uhvaćenih mrežnih paketa po određenim kriterijima
- Filtriranje mrežnih paketa po određenom kriteriju
- Kreiranje statistika o uhvaćenim mrežnim paketima

Iako njegovo ime ne bi tako nalagalo wireshark omogućuje hvatanje paketa i u bežičnim mrežama. Na kojim je sve medijima moguće provesti mrežnu analizu dosta ovisi o operacijskom sistemu na kojem je program instaliran. Pregled medija koje je moguće analizirati ovisno o operacijskom sustavu dan je u tablici 1.1. .

	AIX	**FreeBSD**	**HP-UX**	**Irix**	**Linux**	**Mac OS X**	**NetBSD**	**OpenBSD**	**Solaris**	**Tru64 UNIX**	**Windows**
Fizička sučelja											
ATM					Da	Ne			Da		
Bluetooth	Ne	Ne	Ne	Ne	Da	Ne	Ne	Ne	Ne	Ne	Ne
CiscoHDLC		Da			Da		Da	Da			
Ethernet	Da	Da	Da	Da	Da	Da	Da	Da	Da	Da	Da
FDDI					Da	Ne			Da		

FrameRelay			Ne	Ne	Da	Ne			Ne	Ne	Ne
IrDA	Ne	Ne	Ne	Ne	Da	Ne	Ne	Ne	Ne	Ne	Ne
PPP[2]					Da	Da			Ne		Da
TokenRing	Da	Da		Ne	Da	Ne	Da	Da	Da		Da
USB	Ne	Ne	Ne	Ne	Da	Ne	Ne	Ne	Ne	Ne	Ne
WLAN[4]		Da			Da	Da	Da	Da			Da
Virtualna sučelja											
Loopback		Da	Ne		Da	Da	Da	Da	Ne	Da	
VLAN Tags	Da	Da	Da		Da	Da	Da	Da	Da	Da	Da

Tablica 1.1.

Wireshark isto tako omogućuju unošenje odnosno uvoženje podataka o mrežnim paketima uhvaćenim s drugim programima za mrežnu analizu. Moguće je uvoženje idućih vrsta datotečnih zapisa:

- pcapng.
- libpcap.
- Oracle (prije Sun) *snoop* i *atmsnoop*
- Finisar (prije Shomiti) *Surveyor* hvatanja
- Microsoft *Network Monitor* hvatanja
- Novell *LANalyzer* hvatanja
- AIX *iptrace* hvatanja
- Cinco Networks NetXray hvatanja
- Network Associates Windows-based Sniffer i Sniffer Pro hvatanja
- Network General/Network Associates DOS-based Sniffer hvatanja
- AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/PacketGrabber hvatanja
- RADCOM's WAN/LAN Analyzer hvatanja
- Network Instruments Observer version 9 hvatanja
- Lucent/Ascend izlaz ruter debagiranja
- HP-UX's nettl
- Toshiba's ISDN izlaz ruter debagiranja
- ISDN4BSD *i4btrace*
- Praćenja iz EyeSDN USB S0
- IPLog format iz Cisco Secure Intrusion Detection System

- pppd zapisi (pppdump format)
- Izlaz iz VMS's TCPIPtrace/TCPtrace/UCX$TRACE usluge
- Tekstualni izlaz iz DBS Etherwatch VMS usluge
- Visual Networks' Visual UpTime mrežna hvatanja
- Izlaz iz CoSine L2 debug
- Izlaz iz Accellent's 5Views LAN agenata
- Endace Measurement Systems' ERF format hvatanja
- Linux Bluez Bluetooth stogovni hcidump -w zapisi
- Catapult DCT2000 .out datoteke
- Gammu generiran teksutalni izlaz iz Nokia DCT3 phones in Netmonitor mode
- IBM Series (OS/400) Comm traces (ASCII & UNICODE)
- Juniper Netscreen snoop hvatanja
- Symbian OS btsnoop hvatanja
- Tamosoft CommView hvatanja
- Textronix K12xx 32bit .rf5 format hvatanja
- Textronix K12 tekstualni format hvatanja
- Apple PacketLogger hvatanja
- Hvatanja iz Aethra Telecommunications' PC108 software

Pakete uhvaćene wireshark alatom moguće je i trajno pohraniti u nekom od idućih formata:

- pcapng (*.pcapng).
- libpcap, tcpdump
- Accellent 5Views (*.5vw)
- HP-UX's nettl (*.TRC0,*.TRC1)
- Microsoft Network Monitor - NetMon (*.cap)
- Network Associates Sniffer - DOS (*.cap,*.enc,*.trc,*fdc,*.syc)
- Network Associates Sniffer - Windows (*.cap)
- Network Instruments Observer verzija 9 (*.bfr)
- Novell LANalyzer (*.tr1)
- Oracle (prije Sun) snoop (*.snoop,*.cap)
- Visual Networks Visual UpTime promet (*.*)

Performanse svih prethodno navedenih opcija tj. funkcionalnosti dosta ovise o radnom okruženju unutar kojeg se Wireshark koristi. Na performanse najviše utječe veličina uhvaćenih mrežnih paketa koji se analiziraju. Ukoliko njihova veličina premašuje memorijske kapacitete sustava program će se srušiti. Važno je napomenuti da iako Wireshark za hvatanje paketa koristi odvojene dretve glavno sučelje je jednodretveno što kao posljedicu ima nemogućnost poboljšanja performansi programa u višejezgrenim okruženjima

Važno je još napomenuti da Wireshark ne omogućuje detekciju invazivnih događanja u mreži, ali može pomoći u njihovom otkrivanju. Isto tako Wireshark-om se ne može djelovati u mreži odnosno odašiljati pakete po mreži. Možemo zaključiti kako je Wireshark promatrač mreže, a ne njen aktivni sudionik.

2. Izgradnja i instaliranje programa Wireshark

Za instalaciju Wireshark-a na Windowse ili Mac OS X dovoljno je otići na: https://www.wireshark.org/download.html te preuzeti odgovarajuću instalaciju i pokrenuti ju.

Ukoliko se Wireshark instalira na neki drugi operativni sustav najbolja opcija je instalacija iz izvornog koda. Iako mnogi operativni sustavi imaju u sebi izvorno instaliran Wireshark često je verzija dobivena s operativnim sustavom zastarjela pa je stoga bolje instalirati novu verziju. Proces instalacije je moguće podijeliti u tri osnovna koraka:

1. Preuzeti izvorni kod ili binarni zapis trenutne verzije
2. Ukoliko se skine izvorni kod potrebno ga je kompajlirati u binarni zapis
3. Instalacija binarnog koda na odabranoj lokaciji

Preuzimanje izvornog koda i njegovog binarnog zapisa moguće je na adresi: https://www.wireshark.org/ .

2.1. Instalacija na UNIX sustav

Instalaciju na UNIX sustav moguće je podijeliti u 5 koraka:

1. Ukoliko se izvorni kod nalazi u zip datoteci potrebno ga je raspakirati. To je izvedivo pomoću naredbe:
   a. $ tar xaf wireshark -2.0.5.tar.bz2
      Za UNIX i Linux sustave koji koriste GNU tar.
   b. $ bzip2 –d wireshark-2.0.5.tar.bz2
      $ tar xf wireshark-2.0.5. tar
      Za ostale UNIX sustave

2. Nakon toga potrebno se pozicionirati na Wireshark direktorij s izvornim kodom što se radi naredbom:
   a. $ wireshark-2.0.5

3. Prije izgradnje izvornog koda potrebno ga je konfigurirati za trenutni UNIX sustav što se provodi naredbom:
   a. $ ./configure

4. Potom se izvorni kod izgradi naredbom:
   a. $ make

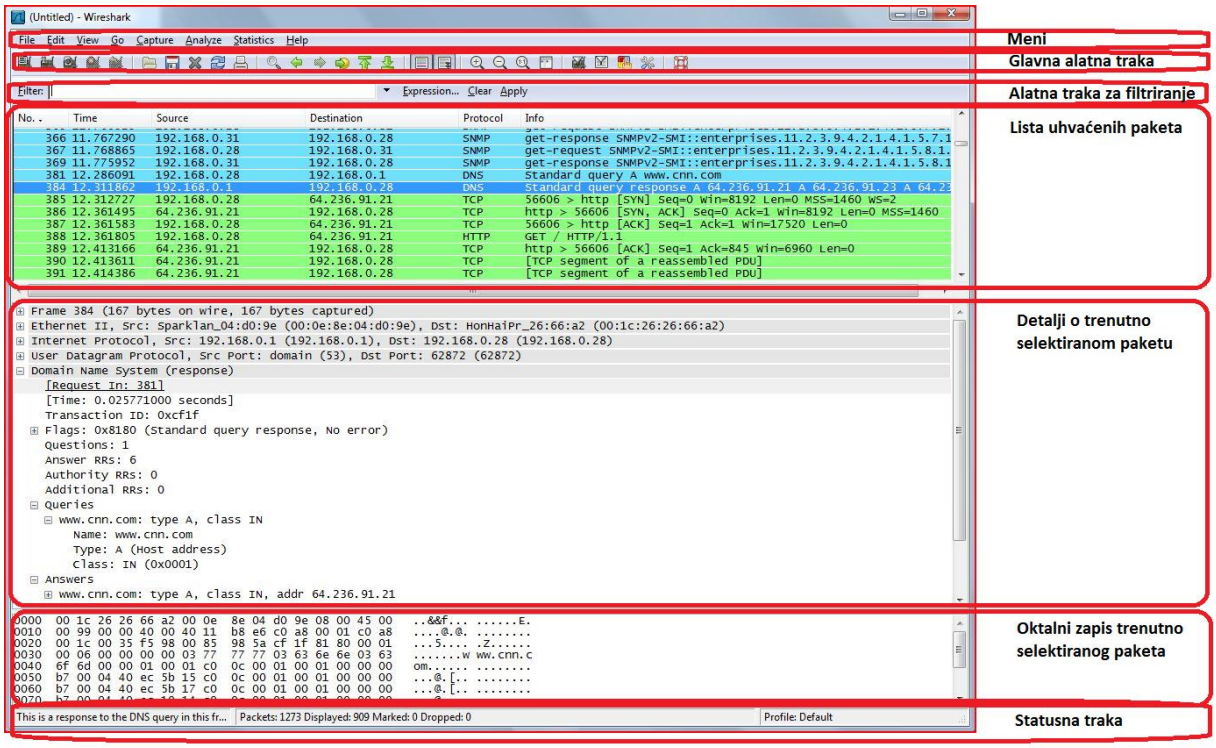
5. Te se konačno instalira na željenu lokaciju naredbom:
    a. $ make install

Nakon provođenja navedenih koraka program je spreman za korištenje.

3. Grafičko sučelje

Izgled glavnog prozora prilikom analize uhvaćenih paketa prikazan je na slici 3.1. Glavni prozor možemo podijeliti na 7 logičkih cjelina:

1. Meni- služi za pokretanje akcija
2. Glavna alatna traka- pruža brzi pristup često korištenim alatima
3. Alatna traka za filtriranje
4. Lista uhvaćenih paketa
5. Lista detalja o trenutno selektiranom paketu
6. Oktalan zapis trenutno selektiranog paketa
7. Statusna traka



3.1.-Grafičko sučelje Wireshark alata

3.1. Meni

Meni omogućuje iduće opcije:

- File – pruža mogućnosti otvaranja i spajanja različitih datoteka te spremanja, ispisa i izvoženja kompletnih ili dijelova uhvaćenih paketa odnosno datoteka. Pruža mogućnost terminiranja programa.
- Edit – pruža mogućnosti traženja paketa, njihovog referenciranja i vremenskog označavanja. Omogućuje i podešavanje konfiguracije programa i postavljanje vlastitih preferenci u programu.
- View – omogućuje kontrolu prikaza uhvaćenih paketa
- Go – pruža opciju pozicioniranja na određeni paket
- Capture – pruža mogućnosti pokretanja i zaustavljanja hvatanja paketa te podešavanja filtriranja paketa koji se hvataju
- Analyze – pruža mogućnosti prikaznih filtara, omogućavanje odnosno onemogućavanje analize protokola te konfiguriranje korisničkih dekodiranja uhvaćenih paketa i praćenje TCP protoka.
- Statistics – omogućuje prikaz raznih statistika o uhvaćenim paketima te prikaz protokolarne hijerarhije
- Telephony – pruža mogućnosti prikaza raznih statistika vezanih uz telefoniju.
- Internals – pruža informacije o unutrašnjim funkcioniranjima samog Wireshark alata
- Help – pruža korisniku pomoć pri korištenju alata

3.2. Glavna alatna traka

Kao što je rečeno glavna alatna traka pruža brzi pristup često korištenim alatima. Glavna alatna traka pruža funkcionalnosti navedene u tablici 3.1. .

Ikona u alatnoj traci	**Ime stavke alatne trake**	**Pristup istoj stavci preko meni-a**	**Opis**
	**Interfaces…**	**Capture →Interfaces…**	Pokreće CIL(Capture Interface List) prozor.
	**Options…**	**Capture →Options…**	Omogućuje postavljanje postavki za hvatanje paketa te pokretanje hvatanja.
	**Start**	**Capture →Start**	Služi za pokretanje hvatanja paketa po trenutnim postavkama.
	**Stop**	**Capture →Stop**	Služi za zaustavljanje hvatanja paketa.

Ikona u alatnoj traci	Ime stavke alatne trake	Pristup istoj stavci preko meni-a	Opis
	**Restart**	**Capture →Restart**	Zaustavi trenutni proces hvatanja paketa te pokrene novi.
	**Open…**	**File → Open…**	Omogućuje učitavanje datoteke s prije uhvaćenim paketima.
	**Save As…**	**File → Save As…**	Omogućuje spremanje trenutno uhvaćenih paketa u datotečnom obliku.
	**Close**	**File → Close**	Omogućuje prekidanje i zatvaranje trenutnog hvatanja paketa.
	**Reload**	**View → Reload**	Omogućuje ponovno učitavanje zatvorene datoteke s uhvaćenim paketima.
	**Print…**	**File → Print…**	Omogućuje ispis zapisa o svim trenutno uhvaćenim paketima.
	**Find Packet…**	**Edit → Find Packet…**	Pokreće prozor za traženje specifičnog paketa.
	**Go Back**	**Go → Go Back**	Omogućuje pomicanje unazad po paketima.
	**Go Forward**	**Go → Go Forward**	Omogućuje pokretanje unaprijed po paketima.
	**Go to Packet…**	**Go → Go to Packet…**	Pokreće prozor za pozicioniranje na određeni paket.
	**Go To First Packet**	**Go → First Packet**	Pozicionira korisnika na prvi uhvaćeni paket.
	**Go To Last Packet**	**Go → Last Packet**	Pozicionira korisnika na zadnji uhvaćeni paket
	**Colorize**	**View →Colorize**	Uključuje odnosno isključuje višebojni prikaz uhvaćenih paketa.
	**Auto Scroll in Live Capture**	**View → Auto Scroll in Live Capture**	Uključuje automatsko pomicanje liste paketa prilikom trenutno aktivnog hvatanja paketa.
	**Zoom In**	**View → Zoom In**	Omogućuje povećanje fonta

Ikona u alatnoj traci	Ime stavke alatne trake	Pristup istoj stavci preko meni-a	Opis
			podataka o uhvaćenom paketu.
	**Zoom Out**	**View** → **Zoom Out**	Omogućuje smanjenje fonta podatka o uhvaćenom paketu
	**Normal Size**	**View** →**Normal Size**	Vraća font podatka o uhvaćenom paketu na početnu veličinu.
	**Resize Columns**	**View** → **Resize Columns**	Prilagođava širinu stupaca koji sadrže podatke o uhvaćenom paketu tako da odgovaraju sadržaju.
	**Capture Filters…**	**Capture** →**Capture Filters…**	Pokreće prozor koji omogućuje konfiguriranje filtara za hvatanje pakte te njihovo pohranjivanje i korištenje prethodno spremljenih konfiguracija.
	**Display Filters…**	**Analyze** →**Display Filters…**	Pokreće prozor koji omogućuje konfiguriranje filtara za prikaz uhvaćenih pakte te njihovo pohranjivanje i korištenje prethodno spremljenih konfiguracija.
	**Coloring Rules…**	**View** →**Coloring Rules…**	Omogućuje korisničko označavanje paketa različitim bojama.
	**Preferences…**	**Edit** →**Preferences**	Pokreće prozor za postavljanje vlastitih postavki.
	**Help**	**Help** →**Contents**	Pokreće prozor za pomoć korisniku u radu.

Tablica 3.1.- Lista stavki glavne alatne trake

3.3. Alatna traka za filtriranje

Alatna traka za filtriranje omogućuje brzo postavljanje postavki vezanih uz prikazne filtre. Alatna traka za filtriranje pruža funkcionalnosti navedene u tablici 3.2. .

Ikona u alatnoj traci	Ime stavke alatne trake	Opis
	**Filter:**	Pokreće prozor s prikazom detalja trenutnog filtra
	Filter input	Služi za unos tekstualnog zapisa po kojem će se filtrirati.
	**Expression…**	Omogućuje ažuriranje prikaznog filtra.
	**Clear**	Resetira trenutni prikazni filtar.
	**Apply**	Primjeni trenutnu vrijednost kao prikazni filtar.

Tablica 3.2. –Lista stavki alatne trake za filtriranje

3.4. Lista uhvaćenih paketa

Lista uhvaćenih paketa prikazuje uhvaćene pakete i bazične informacije o njima te omogućuje selektiranje pojedinačnog paketa. Na slici 3.2. vidimo listu uhvaćenih paketa te naznačene bazične informacije o njima.

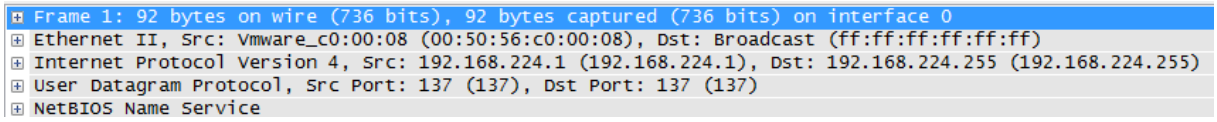
Br. paketa (No. .)	Vrijeme proteklo od početka hvatanja paketa (Time)	Izvorišna IP adresa paketa (Source)	Odredišna IP adresa paketa (Destination)	Protokol prijenosa (Protocol)	Dodatne informacije o paketu (Info)
111	118.726443	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
112	118.835490	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
113	118.869688	66.7.205.168	192.168.0.10	IMAP	Response: \027\003\001\0000\315\365\0
114	118.893955	192.168.0.10	66.7.205.168	IMAP	Request: \027\003\001\000 r\334\330\3
115	118.945312	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
116	119.055345	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
117	119.066296	66.7.205.168	192.168.0.10	IMAP	Response: \027\003\001\0000to\325\212
118	119.103860	192.168.0.10	66.7.205.168	TCP	45200 > imap [ACK] Seq=234 Ack=314 Wi
119	119.166132	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
120	119.275332	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
121	119.386539	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
122	119.495322	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
123	119.605321	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
124	119.715272	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
125	119.826075	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
126	119.935332	192.168.0.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
127	120.183944	192.168.0.10	66.7.205.168	TCP	38636 > http [FIN, ACK] Seq=7308 Ack=

3.2.-Primjer liste uhvaćenih paketa

3.5. Lista detalja o trenutno selektiranom paketu

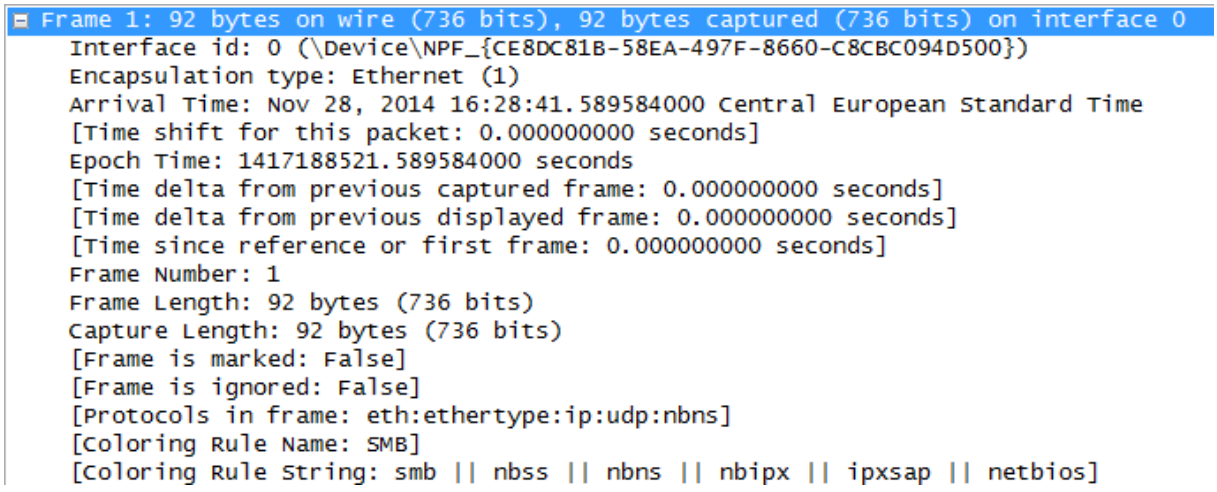
U ovoj listi očekivano se nalaze detaljni podaci o trenutno selektiranom paketu. Tu se nalazi programska interpretacija podataka u uhvaćenom paketu. Lista sadrži pet polja, a to su:

1. Polje o okviru
2. Polje o protokolu transportnog sloja
3. Polje o protokolu mrežnog sloja
4. Polje o protokolu sloja podatkovne poveznice
5. Polje o podacima vezanim uz NetBIOS nazivnu uslugu.

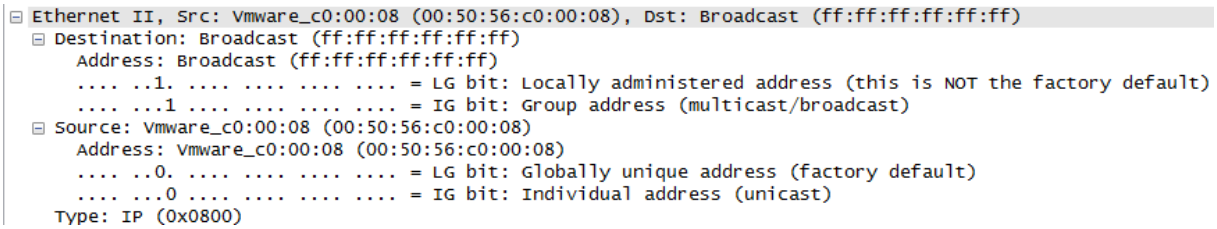


3.3.-Primjer liste detalja o trenutno selektiranom paketu

Kao što je vidljivo iz slike 3.3. svako polje je moguće ekspandirati za njegov detaljniji prikaz odnosno sakriti ukoliko njegov sadržaj trenutno nije od interesa. Detaljan prikaz polja vidljiv je na slikama 3.4.-3.8. .



3.4.-Polje općih podataka o uhvaćenom paketu



3.5.-Polje podataka vezanih uz sloj podatkovne poveznice

```
Internet Protocol Version 4, Src: 192.168.224.1 (192.168.224.1), Dst: 192.168.224.255 (192.168.224.255)
  Version: 4
  Header Length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
  Total Length: 78
  Identification: 0x1b02 (6914)
  Flags: 0x00
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0xdd4a [validation disabled]
    [Good: False]
    [Bad: False]
  Source: 192.168.224.1 (192.168.224.1)
  Destination: 192.168.224.255 (192.168.224.255)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
```

3.6.- Polje podataka vezanih uz mrežni sloj

```
User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
    Source Port: 137 (137)
    Destination Port: 137 (137)
    Length: 58
  Checksum: 0xc153 [validation disabled]
      [Good Checksum: False]
      [Bad Checksum: False]
    [Stream index: 0]
```

3.7.- Polje podatka vezanih uz transportni sloj

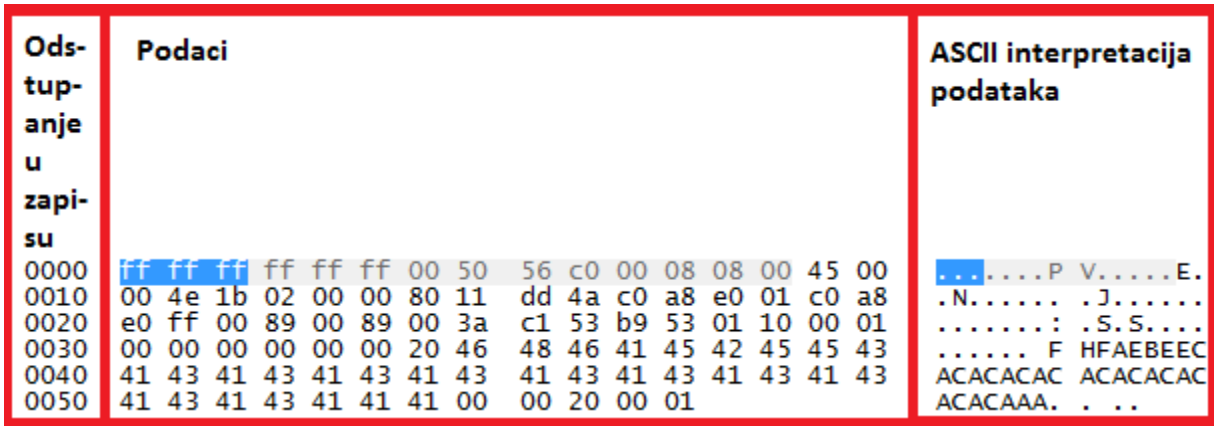
```
NetBIOS Name Service
    Transaction ID: 0xb953
  Flags: 0x0110 (Name query)
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Name query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... ...1 .... = Broadcast: Broadcast packet
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    WPAD<00>: type NB, class IN
        Name: WPAD<00> (Workstation/Redirector)
        Type: NB
        Class: IN
```

3.8.- Polje podataka vezanih uz sesijski sloj

Iako je značenje sadržaja ovih polja važno za razumno korištenje Wireshark alata ono nije primaran fokus ovo teksta stoga se čitatelja zainteresiranog za značenje detalja u prikazu polja upućuje na : [3] i [4].

3.6. Oktalan zapis trenutno selektiranog paketa

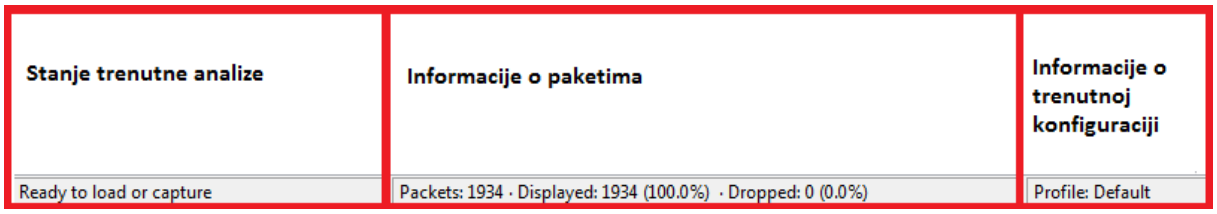
U ovom polju nalazi se oktalan zapis podataka trenutno selektiranog paketa, lijevo od podataka navedeno je odstupanje podataka u zapisu, a desno se nalazi ASCII interpretacija podataka. Ukoliko Wireshark detektira povezanost više paketa u ovom polju će biti prikazan sadržaj svih tih paketa spojenih u jednu logičku cjelinu. Primjer podatkovnog polja prikazan je na slici 3.9. .



3.9.- Primjer oktalna zapisa trenutno selektiranog paketa

3.7. Statusna traka

Statusna traka prikazuje status trenutne analize paketa. S lijeve strane se prikazuje stanje trenutne analize, u sredini se nalaze informacije o broju paketa te njihovom prikazu, skroz desno se nalaze informacije o trenutno korištenoj konfiguraciji za analizu paketa. Primjer statusne trake vidljiv je na slici 3.10. .



3.10.- Primjer statusne trake

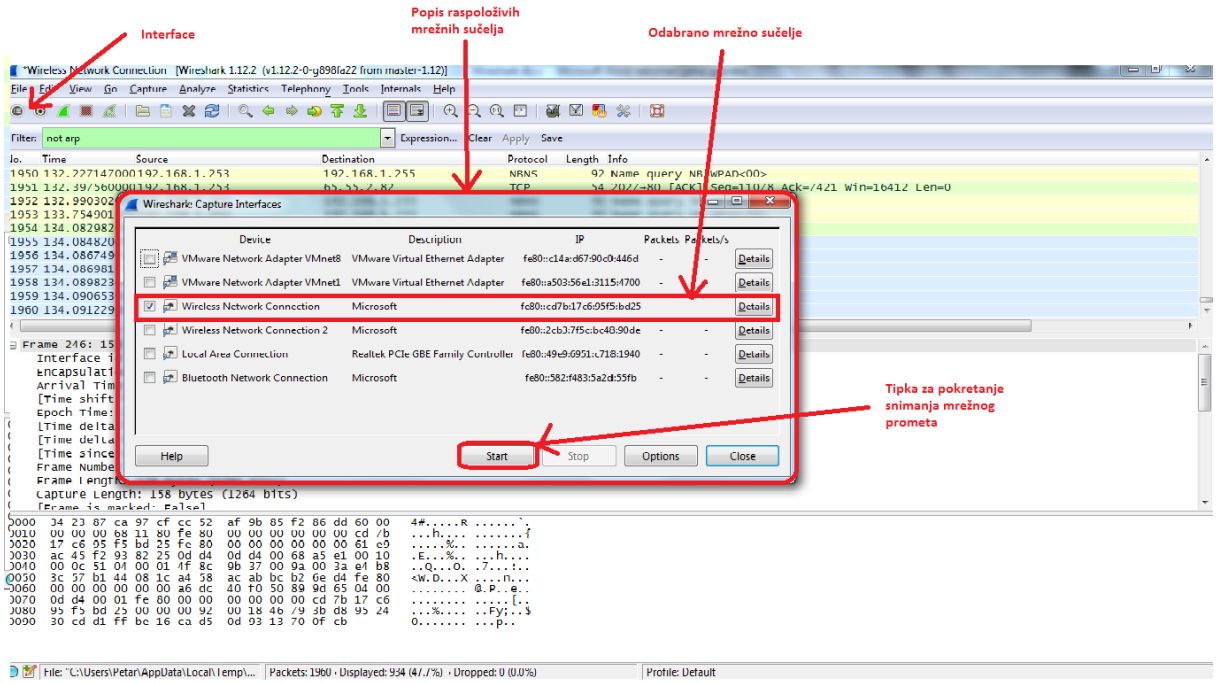
Jedina moguća interakcija s statusnom trakom je na skroz desnom polje. Ukoliko se pritisne da njega podiže se prozor za podešavanje trenutne konfiguracije korištene u analizi.

4. Hvatanje mrežnih paketa

Hvatanje trenutnog mrežnog prometa je središnja funkcija Wireshark alata. Glavne funkcionalnosti koje pruža Wireshark alat za hvatanje paket su:

- Hvatanje prometa na fizički različitim medijima prijenosa
- Zaustavljan je hvatanja ovisno o predodređenim događajima kao što su: Količina uhvaćenih podataka, proteklo vrijeme te broj uhvaćenih paketa.
- Prikaz dekodiranih paketa tijekom hvatanja drugih
- Filtriranje paketa ovisno o postavljenim parametrima
- Pohrana uhvaćenog sadržaja za buduću analizu
- Istovremeno hvatanje podataka na više mrežnih sučelja

Kako bi se pokrenulo hvatanje paketa potrebno je osigurati potrebna dopuštenja odnosno pravo na hvatanje paketa na zadatom mjestu u mreži te je potrebno ispravno odabrati mrežno sučelje preko kojeg prolaze podaci od interesa. Odabir mrežnog sučelja najlakše je izvesti pritiskom na ikonu Interface u glavnoj alatnoj traci. Nakon odabira sučelja dovoljno je pritisnuti tipku start kako bi se počeo hvatati mrežni promet. Spomenuti elementi istaknuti su na slici 4.1. .



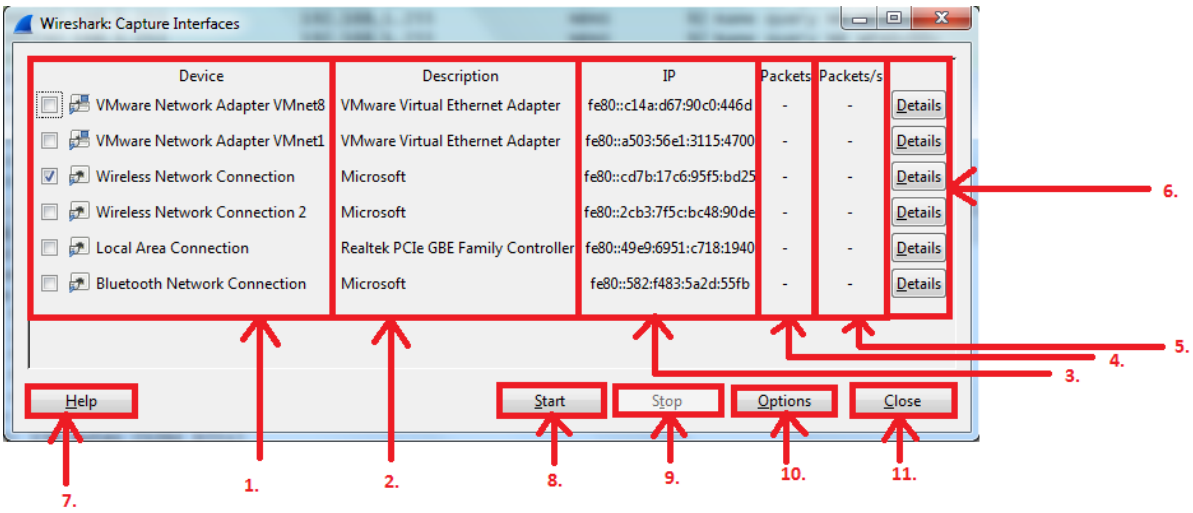
4.1.- Primjer osnovnih funkcionalnosti prilikom hvatanja paketa

Ukoliko se želi pratiti promet na više mrežnih sučelja dovoljno je u listi mrežnih sučelja odabrati odnosno označiti više sučelja. Naočigled ovaj postupak izgleda vrlo jednostavno, ipak za efikasno korištenje alata potrebno ga je raščlaniti na dijelove te se sa svakim dijelom pokretanja detaljnije upoznati.

4.1. Izbor mrežnog sučelja

Iako su same osnove izbora mrežnog sučelja navedene potrebno se detaljnije upoznati s prozorom koji nudi listu raspoloživih mrežnih sučelja. Prozor se može podijeliti na iduće dijelove:

1. Popis raspoloživih / vidljivih sučelja
2. Opis raspoloživih / vidljivih sučelja
3. IP adresa raspoloživih / vidljivih sučelja
4. Broj paketa uhvaćenih po sučelju
5. Broj paketa uhvaćenih po sučelju u zadnjoj sekundi
6. Tipka za pregled detalja sučelja
7. Tipka za pomoć pri korištenju alata
8. Tipka za započinjanje hvatanja paketa
9. Tipka za završavanje hvatanja paketa
10. Tipka za podešavanje opcija vezanih uz hvatanje paketa
11. Tipka za zatvoriti prozor s listom sučelja

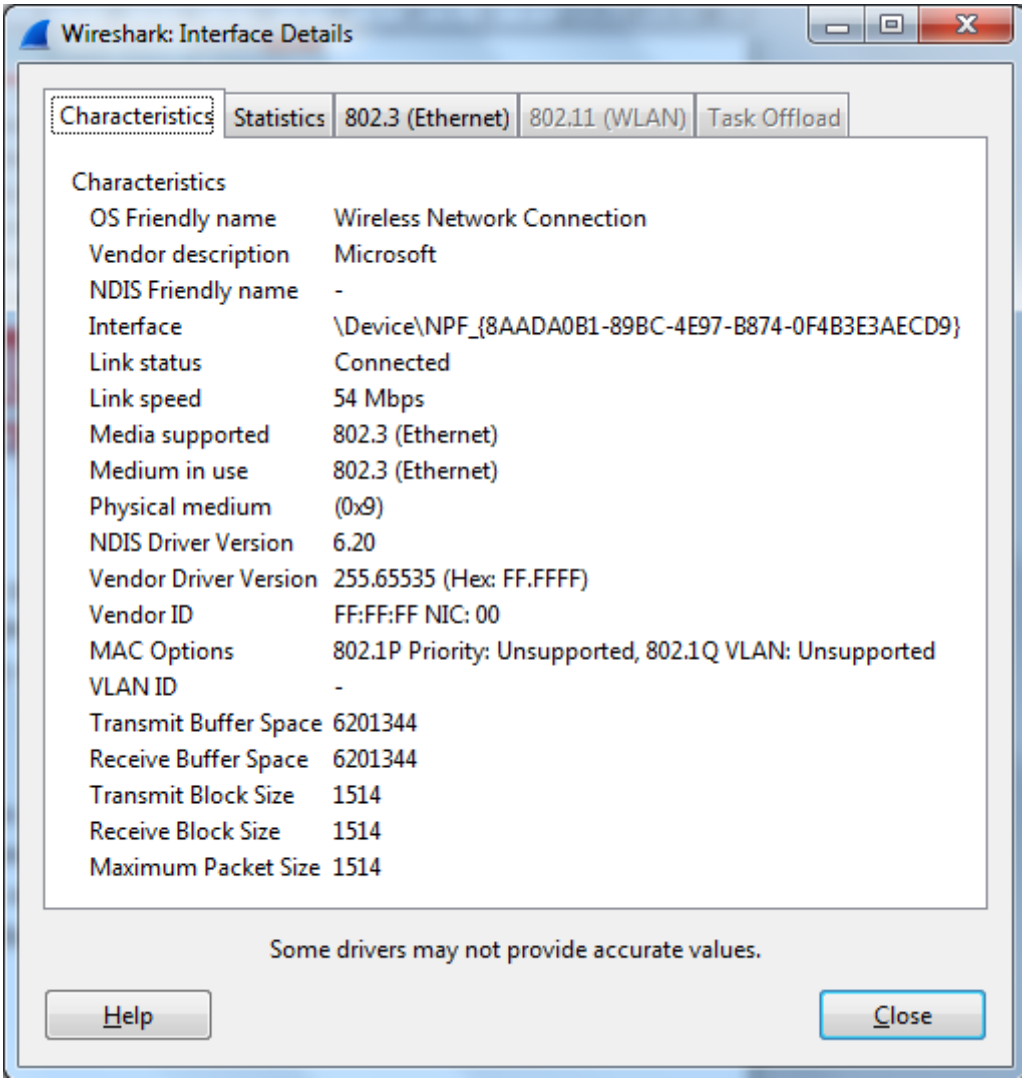


4.2.- Prozor s listom raspoloživih mrežnih sučelja

Većina navedenih dijelova je intuitivno shvatljiva i nije potrebna njihova detaljnija analiza. Od navedenih dijelova posebno su zanimljivi tipka za pregled detalja sučelja te tipka za podešavanje opcija vezanih uz hvatanje paketa, a za rad s Wireshark alatom izuzetno je korisno dobro poznavanje opcija vezanih uz hvatanje paketa.

4.1.1. Detalji sučelja

Detaljima sučelja moguće je pristupiti pritiskom na tipku Details u prozoru za izbor mrežnog sučelja. Prilikom pritiska otvara se prozor s informacijama o sučelju. U prozor je moguć pregled općih karakteristika mrežnog sučelja, pregled statistike rada odabranog sučelja i pregled protokola koji se odvijaju na odabranom sučelju. Detalji navedeni u ovom prozoru mogu biti korisni prilikom dubinske analize događanja u mreži. Primjer prozora s detaljima sučelja prikazan je na slici 4.3. .

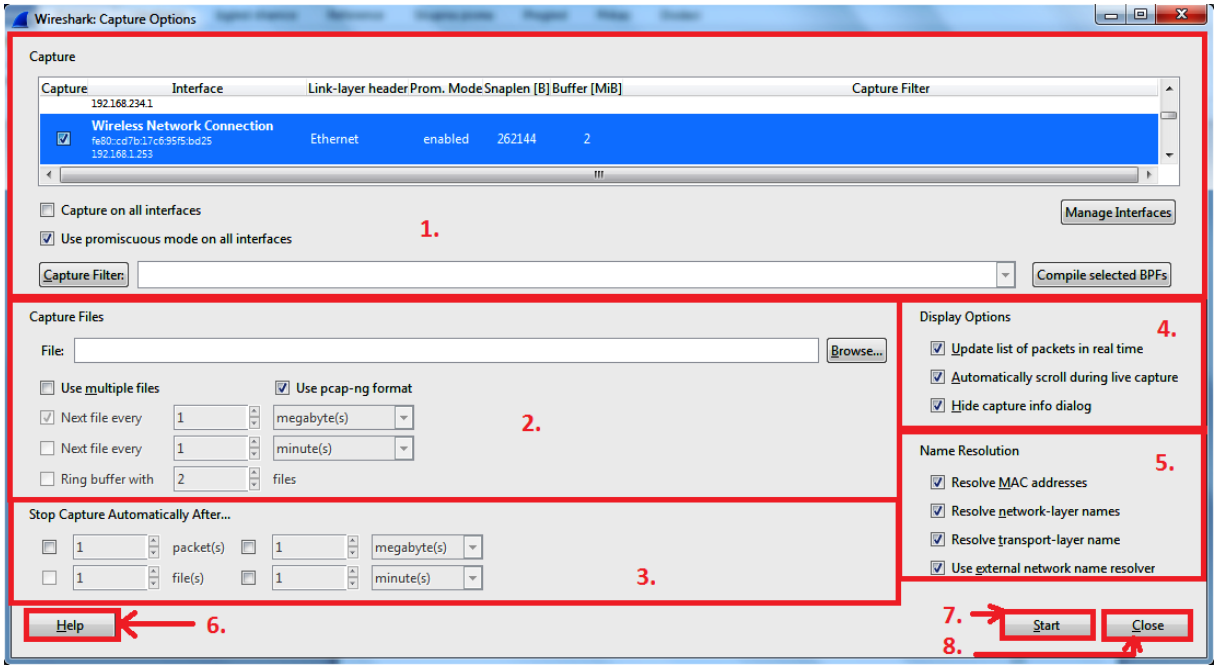


4.3.- Prozor s detaljima sučelja

4.1.2 Podešavanje opcija za hvatanje paketa na određenom sučelju

Kako bi se pristupilo podešavanju opcija vezanih uz hvatanje paketa na određenom sučelju prilikom odabira tog sučelja u prozoru s listom sučelja potrebno je pritisnuti tipku za podešavanje opcija vezanih uz hvatanje paketa. Pritiskom na spomenutu tipku otvara se prozor vidljiv na slici 4.4. . Prozor se sastoji od pet okvira te tri tipke koje ne pripadaju ni jednom od njih:

1. Capture okvir
2. Capture Files okvir
3. Stop Capture okvir
4. Display Options okvir
5. Name Resolution okvir
6. Help tipka
7. Start tipka
8. Cancle tipka

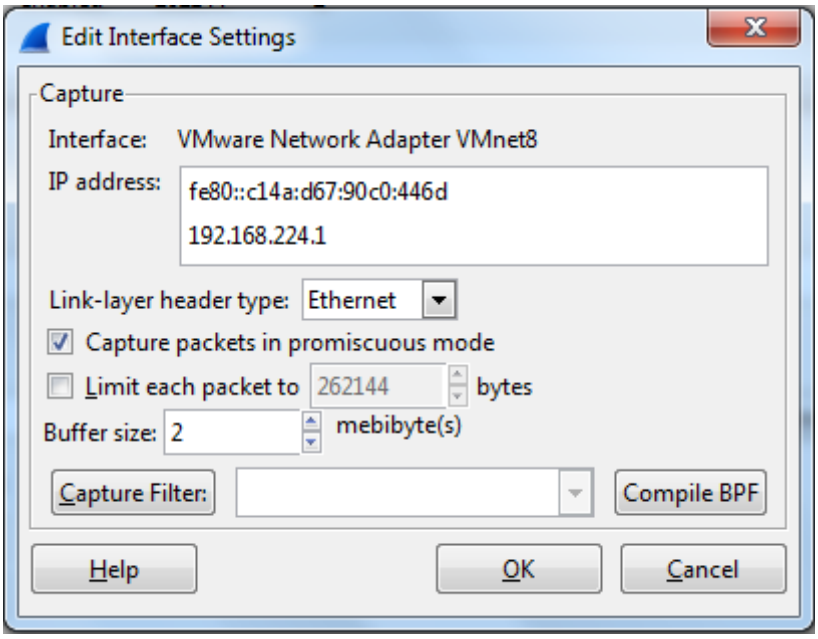


4.4.- Prozor za podešavanje opcija hvatanja

Prvi element Capture okvira je tablica koja prikazuje:

- Ime, IP i MAC adresu sučelja
- Tip zaglavlja u sloju podatkovne poveznice
- Informacije da li je promiskuitetan mod omogućeni ili ne
- Maksimalnu količinu podataka koja će biti uhvaćena po pojedinom paketu
- Veličinu buffera zauzetog za spremanje uhvaćenih podataka
- Odabrani filtar prilikom hvatanja

Tablica nudi mogućnost odabira sučelja na kojem se želi provoditi hvatanje paketa. Ukoliko se dva puta klikne na sučelje navedeno u tablici tada će se otvoriti prozor za podešavanje sučelja, vidljiv na slici 4.5. . Unutar ovo paketa moguće je postaviti filtre na sučelje, omogućiti hvatanje promiskuitetnih paketa koji pristižu na sučelje te promijeniti veličinu paketa koji se mogu hvatati.



4.5.- Prozor za podešavanje sučelja

Nakon tablice sučelja nalaze se tipke kojima se omogućuje odnosno onemogućuje hvatanje na svim sučeljima i hvatanje svih paketa u promiskuitetnom modu. Ispod njih se nalazi polje za unos filtra uhvaćenih paketa i tipka koja omogućuje kompajliranje filtra za hvatanje paketa u BPF kod. Spomenuta tipka otvara prozor s dobivenim BPF kodom. Posljednji element Capture okvira služi za otvaranje prozora koji dozvoljava upravljanje sučeljima. Unutar ovog prozora moguće je dodavati cjevovode, identificirati i skrivati sučelja te dodavati udaljena sučelja.

Nakon Capture okvira slijedi Capture Files okvir koji nudi funkcionalnosti upravljanja datotekama koje sadrže podatke o uhvaćenim paketima. Moguće je navesti ime datoteke u koju će se pohranjivati uhvaćeni podaci tj. iz koje će se učitati uhvaćeni podaci. Ukoliko se ne navede ime datoteke tada Wireshark koristi privremenu datoteku za pohranu trenutnih podataka. Ako se označi polje za korištenje više datoteka tada će program na određeni događaj početi spremati podatke u drugu datoteku. Postavljanje ovih događaja omogućeno je odmah ispod polja koje specificira korištenje više datoteka. Mogući događaji su uhvaćena određena količina podataka ili istek zadatog vremena. Uz to moguće je specificirati veličinu kružnog buffera u kojeg će se spremani datoteke. Za format spremanja nudi se pcap-ng

format koji će se automatski primijeniti ukoliko se istovremeno hvataju podaci na više sučelja.

U okviru Stop Capture moguće je navesti uvjete prestanka hvatanja paketa. Uvjeti prestanka mogu biti hvatanje određene količine podataka ili istek zadatog vremena.

Display Options okvir nudi opcije koje za cilj imaju lakše praćenje procesa hvatanja paketa. Preciznije rečeno nudi se opcija za ažuriranje liste uhvaćenih paketa u stvarnom vremenu, opcija za automatsko pomicanje liste uhvaćenih paketa po dolasku novog paketa te opcija za skrivanje prozora s dodatnim informacijama u uhvaćenim paketima.

Name Resolution okvir nudi opcije za automatsko dekodiranje identifikacija pronađenih u uhvaćenim paketima. Nude se mogućnosti dekodiranja MAC adresa, IP adresa te adresa transportnog sloja i mogućnost korištenja vanjski specificiranog dekodera adresa.

Tipka Help pruža korisniku pomoć u radu s programom.

Tipka Start pokreće hvatanje paketa s trenutno postavljenim postavkama.

Tipka Cancle zatvara prozor za prozor za podešavanje opcija vezanih uz hvatanje paketa.

4.2. Filtriranje uhvaćenih paketa

Prilikom odabira sučelja moguće je zadati filtriranja paketa. U polja za filtriranja paketa navode se regularni izrazi kojima se ostvaruje željeno filtriranje. Opći oblik ovih regularnih izraza dan je kao:

$$[not]primitiv \left[\frac{and}{or}\right] [not]primitiv \ldots$$

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 adresam odnosno po NetId-u. Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana adresa odredišna odnosno izvorišna.

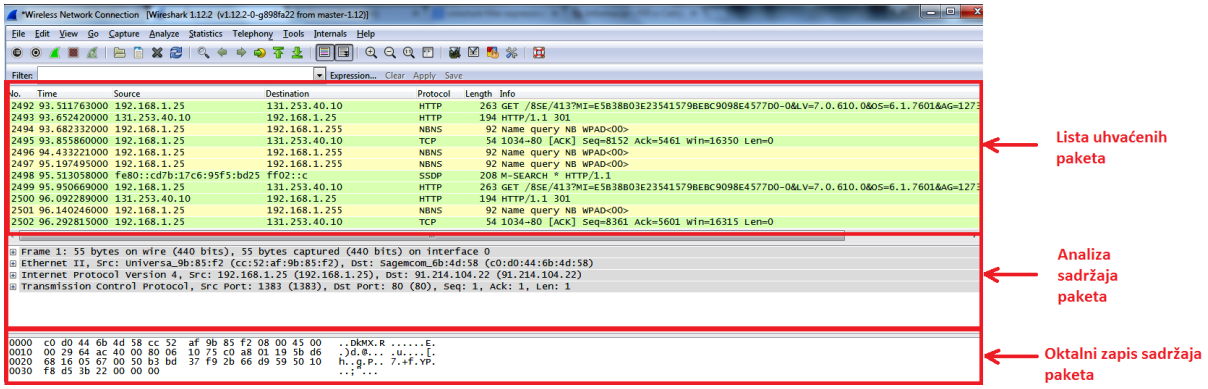
- [tcp/udp] [src/dst] port<port>; Zapis omogućuje filtriranje po protokolu ovisno o tome je li protokol TCP ili UDP. Dodatno je moguće navesti da se filtriranje provodi samo ukoliko je zadana adresa odredišna odnosno izvorišna.
- less/greater <length>; Zapis omogućuje filtriranje paketa čija je veličina 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 višeodredišna ili jednoodredišna.

Za detaljnu analizu sintakse regularnih izraza korištenih za filtriranje čitatelja se upućuje na : http://www.tcpdump.org/manpages/pcap-filter.7.html .

5. Rad s uhvaćenim podacima

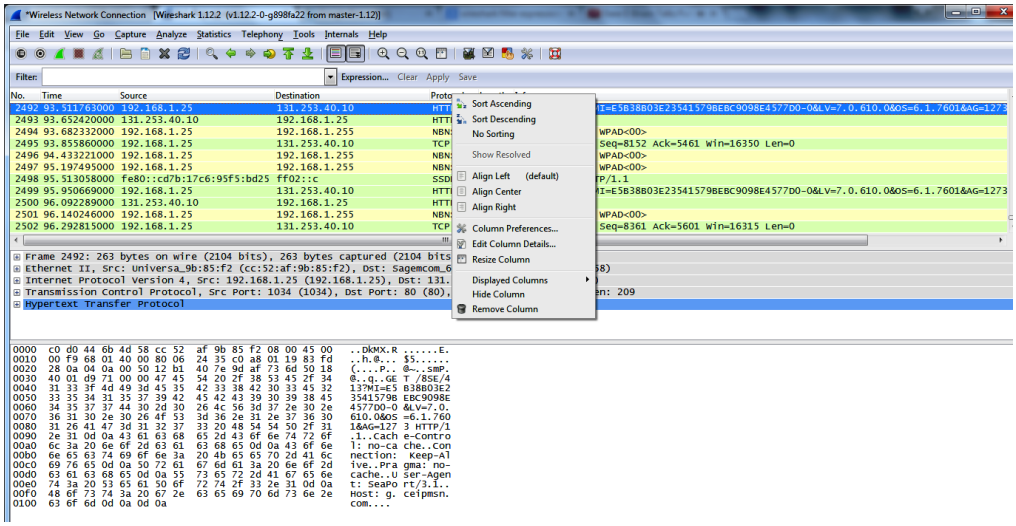
5.1. Opći rad s uhvaćenim paketima

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.



5.1.- Primjer grafičkog sučelja s naglašenim dijelovima za prikaz informacija o uhvaćenim paketima

Desnim klikom na element liste paketa ili na ime stupca u prikazu uhvaćenih paketa nude se dodatne opcije za rad s paketima. Prikaz opcija ponuđenih desnim klikom na ime stupca prikaza uhvaćenih paketa dan je na slici 5.2. .



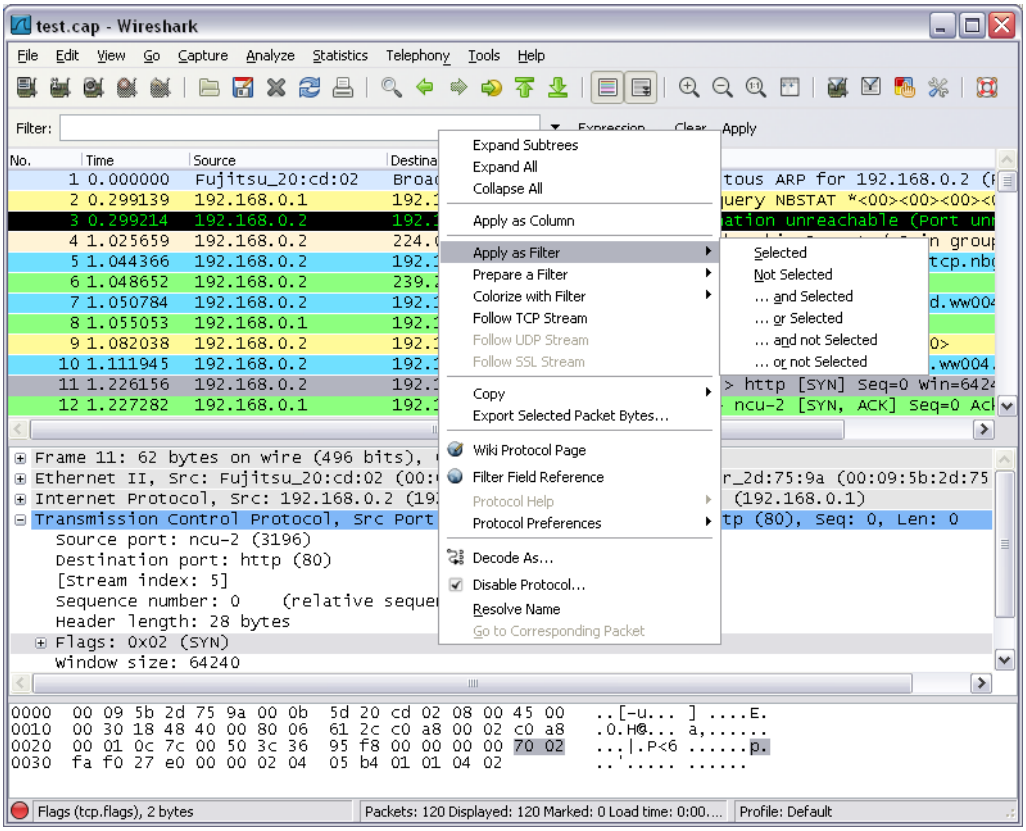
5.2.- Opcije ponuđene desnim klikom na ime stupca liste uhvaćenih elemenata

Funkcionalnosti ponuđenog izbornika objašnjene su u tablici 5.1. .

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

Tablica 5.1.- Popis funkcionalnosti izbornika za rad
s stupcima u listi uhvaćenih paketa

Prikaz opcija ponuđenih desnim klikom na element liste uhvaćenih paketa prikazan je na slici 5.3. .



5.3.- Opcije ponuđene desnim klikom na uhvaćeni element

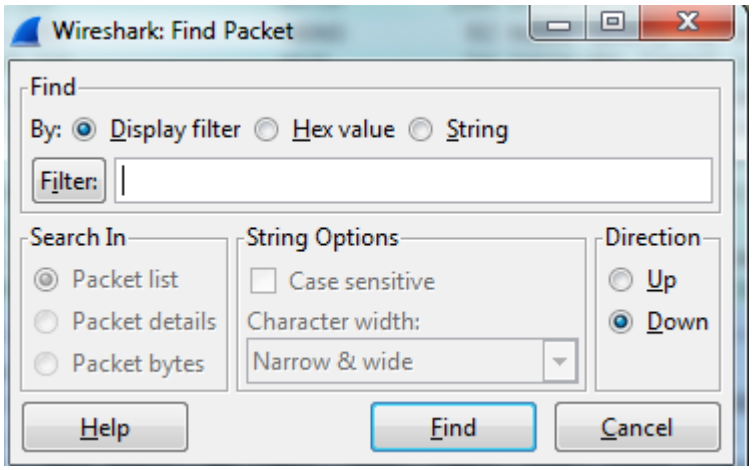
Funkcionalnosti ponuđenog izbornika objašnjene su u tablici 5.2. .

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

Stavka	Opis
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.
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.

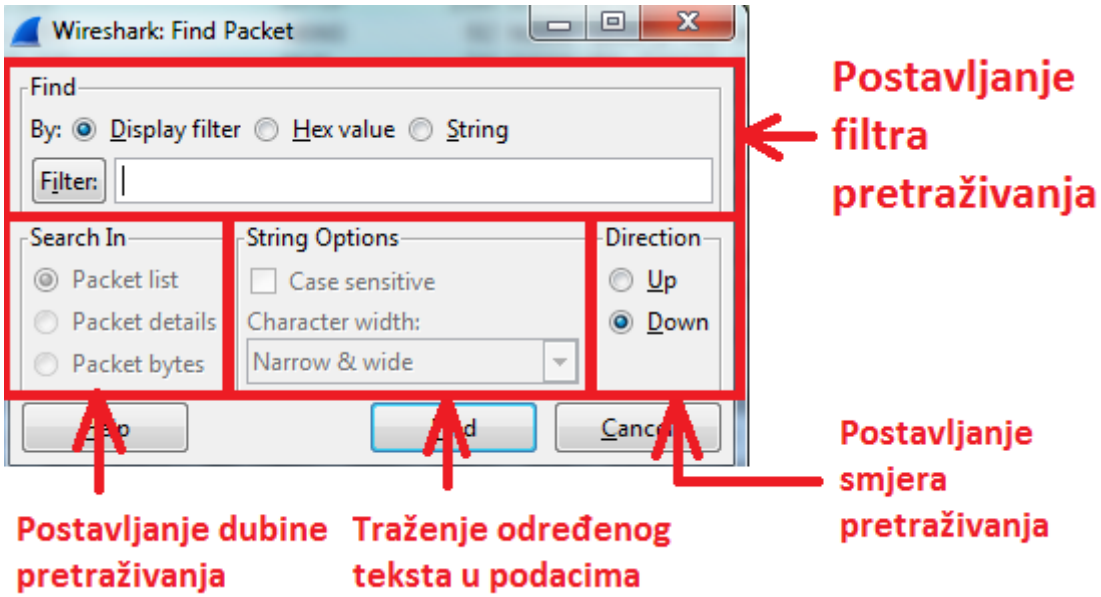
Tablica 5.2.- Popis funkcionalnosti izbornika za
rad s elementima u listi uhvaćenih paketa

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 ovog prozora dan je na slici 5.4. .



5.4.-Find Packet prozor

U prozoru je moguće postaviti filtar pretraživanja, područje odnosno dubinu pretraživanja, traženje određenog tekstualnog zapisa u podacima te smjer pretraživanja u listi uhvaćenih paketa.

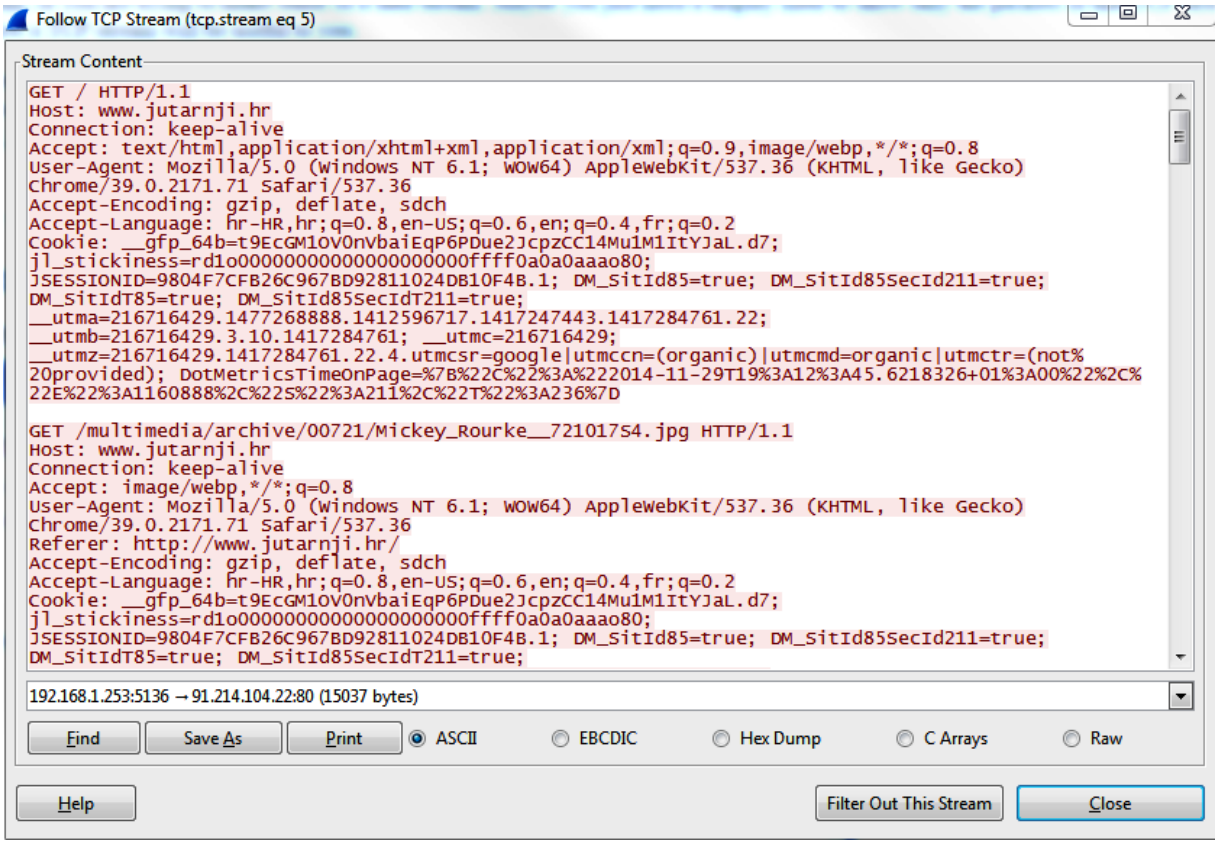


5.5.- Find packet prozor s naznačenim dijelovima

Za pozicioniranje na određeni paket moguće je koristiti i Go to naredbe glavne alatne trake. Go to naredbe će usmjeravati pretraživanje po zadnjim postavljenim postavkama u Find Packet prozoru ili ukoliko nikakve postavke nisu unesene po osnovnim postavkama pretraživanja.

5.2. Praćenje TCP toka

TCP je jedan od osnovnih protokola transportnog sloja. Korištenjem ovog protokola aplikacija stvara virtualni kanal prema odredištu te komunicira preko tog virtualnog kanala. Ovaj protokol se koristi kada je cilj postići podatkovno ispravnu vezu odnosno kada je cilj da svi isporučeni podaci budu točno preneseni kroz komunikacijski kanal. Ukoliko se analiziraju TCP protokoli tumačenje podataka koji se njima prenose može biti od velike pomoći. Wireshark pruža mogućnost praćenja TCP komunikacije te tumačenja njenih podataka na način kako ih tumači aplikacijski sloj. Kako bi se pratio TCP protok informacije dovoljno je na odabrani paket koji primjenjuje TCP protokol kliknuti desni klik te izabrati opciju praćenja TCP komunikacije. Prilikom odabira spomenute opcije pokreće se prozor koji prikazuje podatke razmijenjene u TCP komunikaciji. Primjer ovog prozora dan je na slici 5.6. .

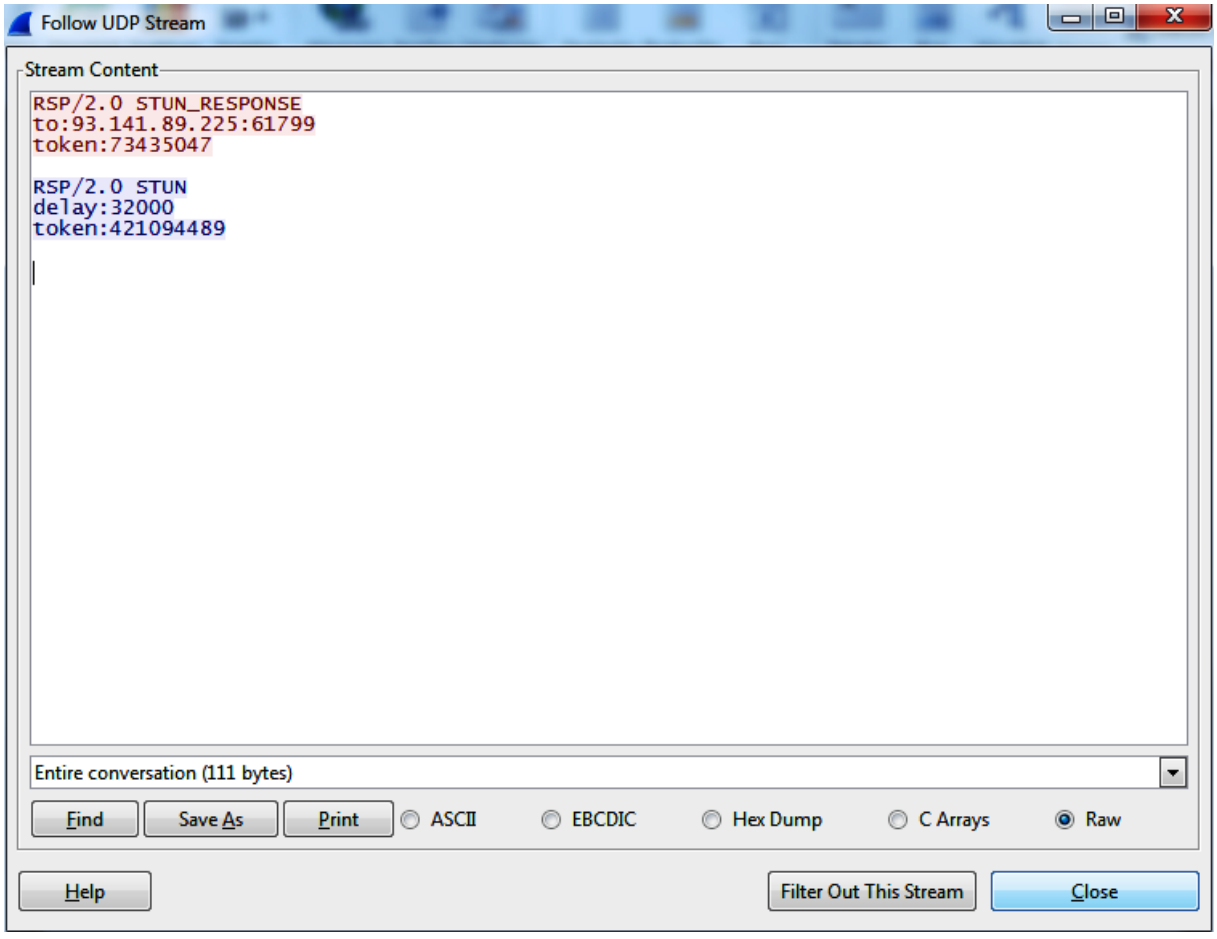


5.6.- Primjer praćenja TCP toka

Podaci prikazani u odabranom TCP toku poredani su redoslijedom kako su se pojavljivali u mreži. Podaci mogu biti prikazani u crvenoj ili plavoj boji ovisno o njihovom smjeru kretanja u komunikaciji.

5.3. Praćenje UDP toka

UDP je jedan od osnovnih protokola transportnog sloja. UDP se koristi za slanje kratkih poruka između entiteta u mreži. Cilj UDP protokola je prijenos informacija u što kraćem vremenu. Za tumačenje podataka poslanih ovim protokolom Wireshark pruža jednaku opciju kao i za TCP protokol. Desnim klikom na izabrani UDP paket te odabirom opcije praćenja UDP toka pokreće se prozor s aplikacijskim prikazom interpretacije podataka razmijenjenih ovim protokolom. Primjer ovog prozora vidljiv je na slici 5.7. .



5.7.-Primjer praćenja UDP toka

Isto kao i kod TCP protokola prikazani podaci su poredani redoslijedom njihova pojavljivanja u mreži te se označavaju crvenom odnosno plavom bojom ovisno o smjer njihovog kretanja u komunikaciji.

6. Wireshark i analiza zloćudnih programa

Wireshark omogućuje detekciju prisutnosti zloćudnih programa. Iako on sam to ne radi na izravan način ukoliko postoji mrežna komunikacija, kada je ne bi trebalo biti, gotovo sigurno se radi o zloćudnom programu koji komunicira s mrežom. Pri analizi zloćudnih programa Wireshark se koristi za detekciju IP adrese s kojom zloćudni program želi komunicirati te identifikaciju podataka koje zloćudni program odašilje. Detekcija IP adrese može izuzetno pomoći pri identifikaciji autora zloćudnog programa, a identifikacija podataka je od velike važnosti pri određivanju djelovanja zloćudnog programa. Identifikacija podataka se provodi praćenjem sumnjivih TCP / UDP tokova. Prilikom analize korisno je prikupiti velike količine podataka potom od spojiti potencijalno kompromitirano računalo s mreže i obaviti analizu.

Sam proces analize dosta ovisi o konkretnom slučaju analize te ga je teško općenito opisati. Jednom kad se ustanovi postojanje zloćudne uporabe mreže idući korak je identificiranje programa koji ju izaziva. U ovu svrhu bolje je korištenje programa kao što je Microsoft Network Monitor koji nudi opciju filtriranja procesa koji komuniciraju s mrežom. Dalje slijedi opća analiza zloćudnog programa koja nije središnja tema ovog teksta.

Primjer izgleda liste uhvaćenih paketa prilikom Torrent komunikacije preko mreže dan je na slici 6.1. .

Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
2013-09-14 20:45:00	192.168.1.110	6881	67.215.242.138	6881	17	ET P2P BitTorrent DHT ping request
2013-09-14 20:47:49	192.168.1.110	49172	131.253.61.86	443	6	PADS New Asset - ssl TLS 1.0 Client Hello
2013-09-14 20:50:20	192.168.1.110	49357	95.215.61.199	80	6	ET P2P possible torrent download
2013-09-14 20:50:33	192.168.1.110	6881	31.172.124.28	80	17	ET P2P Vuze BT UDP Connection (5)
2013-09-14 20:50:42	192.168.1.1	49373	192.168.1.1	80	6	PADS New Asset - unknown @www
2013-09-14 20:50:47	192.168.1.110	6881	109.58.145.211	26651	17	ET P2P BitTorrent DHT nodes reply
2013-09-14 20:50:48	192.168.1.110	6881	65.131.40.116	51413	17	ET P2P BitTorrent DHT announce_peers request
2013-09-14 20:54:01	192.168.1.110	49402	216.151.172.98	6969	6	PADS New Asset - http qBittorrent v3.0.11
2013-09-14 20:54:01	192.168.1.110	49402	216.151.172.98	6969	6	GPL P2P BitTorrent announce request
2013-09-14 20:54:01	192.168.1.110	49402	216.151.172.98	6969	6	ET P2P BitTorrent Announce
2013-09-14 20:54:07	192.168.1.110	49416	67.8.104.234	6890	6	ET P2P BitTorrent peer sync
2013-09-14 20:54:10	219.216.128.25	80	192.168.1.110	49440	6	GPL SHELLCODE x86 NOOP
2013-09-14 20:54:25	95.211.90.142	61066	192.168.1.110	49475	6	ET SHELLCODE Possible Call with No Offset TCP Shellcode
2013-09-14 20:56:34	67.215.238.66	80	192.168.1.110	49595	6	ET INFO EXE - Served Attached HTTP
2013-09-14 20:56:34	67.215.238.66	80	192.168.1.110	49595	6	ET POLICY PE EXE or DLL Windows file download
2013-09-14 20:56:39	192.168.1.110	49655	174.129.220.238	80	6	ET P2P BTWebClient UA uTorrent in use
2013-09-14 20:56:41	192.168.1.110	49657	67.215.246.203	80	6	ET P2P Bittorrent P2P Client User-Agent (uTorrent)
2013-09-14 20:57:15	192.168.1.110	49693	173.241.244.153	80	6	PADS New Asset - http Mozilla/5.0 (MSIE 8.0.7601.17514; Windows...
2013-09-14 20:57:17	46.150.246.120	6881	192.168.1.110	25633	17	ET RBN Known Russian Business Network IP UDP (207)
2013-09-14 21:00:00	91.189.92.163	80	192.168.1.110	49212	6	ET POLICY BitTorrent - Torrent File Downloaded
2013-09-14 21:00:12	192.168.1.110	49223	188.168.58.248	6881	6	GPL P2P BitTorrent transfer
2013-09-14 21:00:34	93.183.218.171	22222	192.168.1.110	25633	17	ET RBN Known Russian Business Network IP UDP (434)

6.1.-Lista uhvaćenih paketa pri Torrent komunikaciji

7. Zaključak

Iz svega navedenog vidljivo je da je Wireshark moćan alat za praćenje događanja u mreži te njihovu analizu. Isto tako je vidljivo da primarna funkcija Wireskark alata nije analiza zloćudnih programa i njihovih djelovanja u mreži, iako može biti izuzetno koristan i u te svrhe. Važno je napomenuti da Wireshark alat pruža više funkcionalnosti nego što je navedeno u ovom tekstu. Za detaljno upoznavanje s Wireshark alatom čitatelja se upućuje na [1]. Smisleno korištenje Wireshark alata zahtijeva od korisnika poznavanje barem osnova komunikacijskih mreža. Iz tog razloga alat korisnicima koji ne poznaju koncepte komunikacijskim mreža može predstavljati nesavladivu zapreku tj. neshvatljiv problem. Za upoznavanje osnova komunikacijskih mreža čitatelja se upućuje na [3] i [4].

8. Literatura

[1] Wireshark ; https://www.wireshark.org/

[2] Fakultet elektrotehnike i računarstva; Radovi iz područja računalne sigurnosti; 2014; http://os2.zemris.fer.hr/index.php?show=start

[3] Ignjac Lovrek, Maja Matijašević, Gordan Ježić, Dragan Jevtić; Komunikacijske mreže; Radna inačica udžbenika v.2.1. Dio 1; 2014;

[4] Vedran Podobnik, Ognjen Dobrijević, Tomislav Grgić, Krunoslav Ivešić; Internetski protokoli u primjeni; Zagreb 2014;