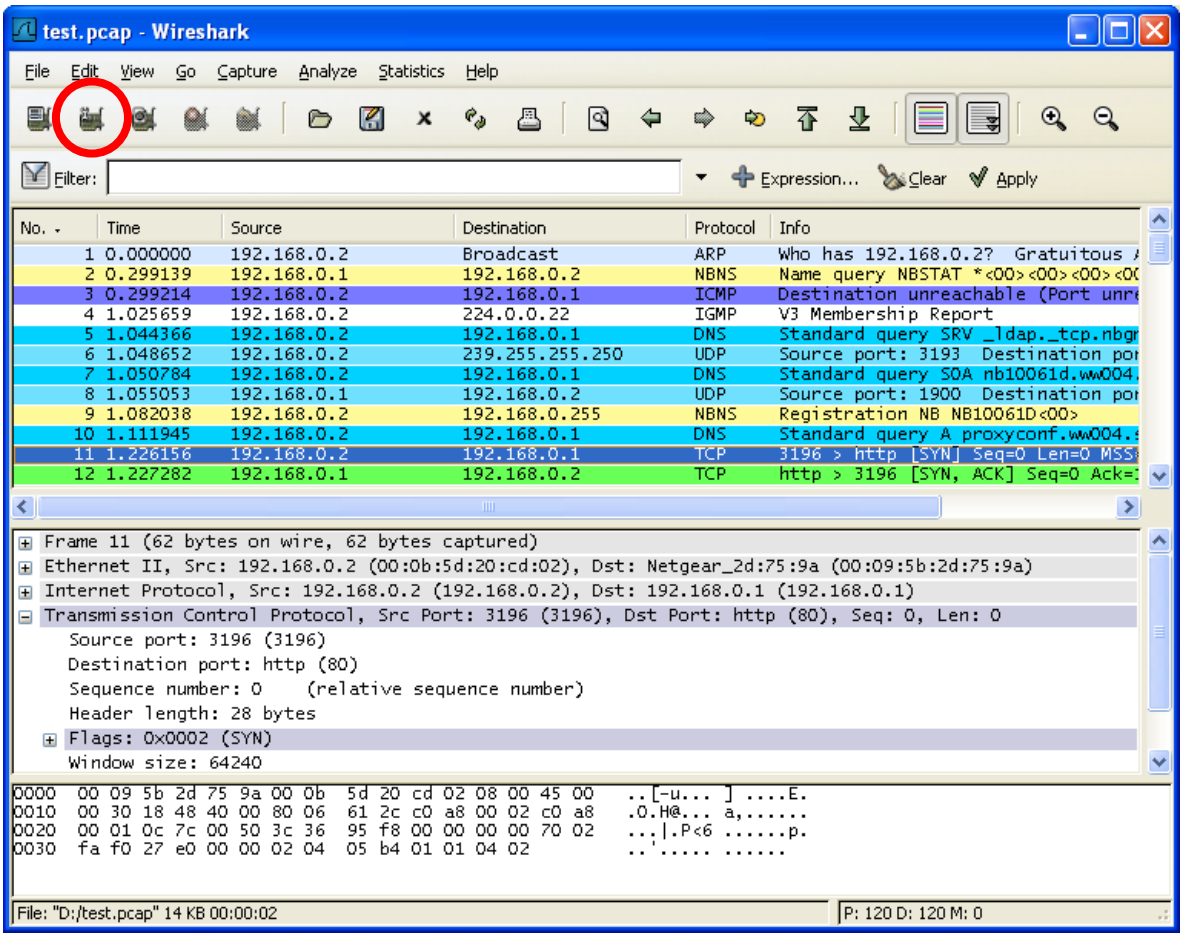
Zajemanje in analiza TCP/IP prometa z orodjem Wireshark

1 Namen

Namen vaje je seznaniti učeče z osnovnimi značilnostmi zajemanja in analize prometa v omrežjih TCP/IP. Izbrano orodje za analizo je aplikacija Wireshark.

2 Opis orodja Wireshark

Orodje Wireshark (http://www.wireshark.org) je izdano pod odprtokodno licenco GNU GPL, kar pomeni, da je prosto dostopno. Wireshark je izjemno zmogljivo in kvalitetno orodje, ki je primerljivo oz. presega podobna komercialna orodja.



Sl. 1: Osnovni izgled grafičnega vmesnika orodja Wireshark

Wireshark omogoča zajem protokolnih podatkovnih enot (ang. Protocol Data Unit - PDU) in analizo prometa. Osnovni pogled v zajeti promet sestavljajo tri okna in sicer:

- okno za prikaz zajetih PDU,
- okno za analizo PDU s prikazanimi podrobnosti PDU-jev in hierarhijo protokolov v protokolnem skladu ter
- okno s prikazano surovo (HEX) vsebino PDU.

Primer s slike št. 1 kaže dekompozicijo sporočila protokola TCP (označeni zajeti PDU je TCP). Iz srednjega dela slike je razvidna hierarhija protokolov, ki si sledi v zaporedju:

Ethernet okvir --> protokol IP --> protokol TCP.

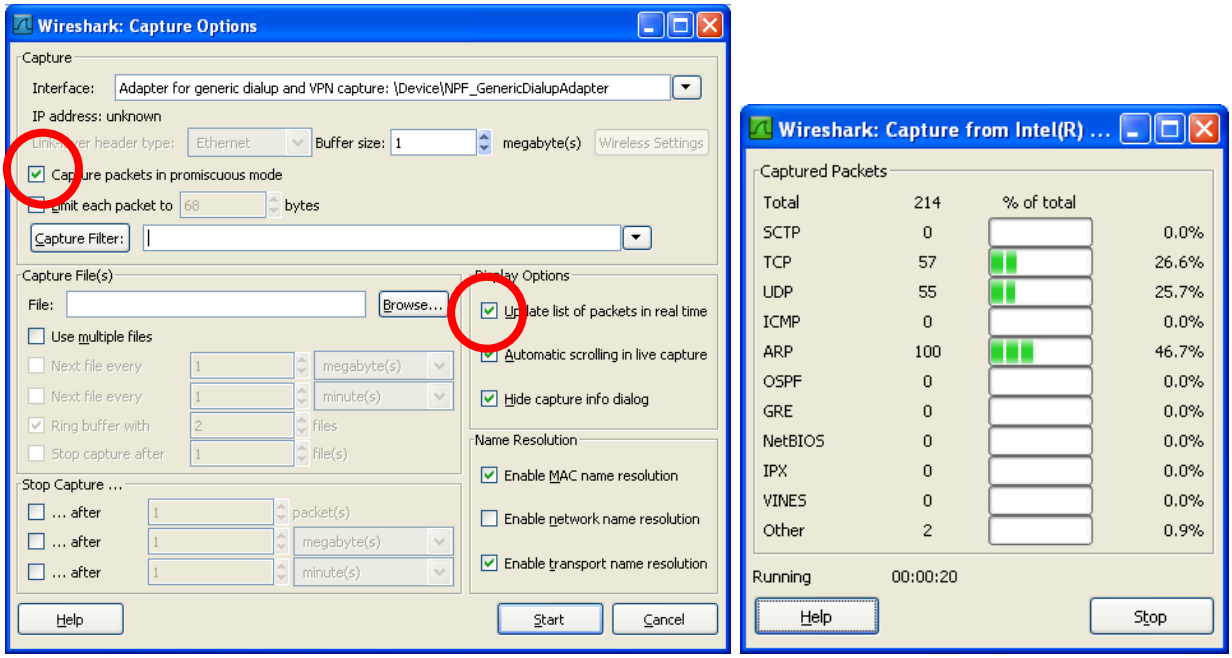
Vsebina višjeležečih protokolov se obravnava kot podatek ter se enkapsulira v nižjeležeče protokole.

2.1 Zajem

Zajem prometa sproži z rdečo barvo označeni gumb na sliki št. 1. Wireshark pozna dva različna načina zajema in sicer:

- normalni zajem in
- promiskuitetni zajem (ang. promiscuous).

Pri navadnem zajemu se zajamejo le sporočila, ki so namenjena **samo gostiteljskemu terminalu** in sporočila tipa **broadcast/multicast**, ki so namenjena vsem terminalom ali skupini terminalov. Vsa ostala sporočila se zavržejo. V promiskuitetnem načinu se zajamejo vsa sporočila, ne glede na ciljni naslov (npr. MAC oz. IP), če so vsi terminali na skupnem mediju.



Sl. 2: Nastavitve za zajem prometa (določanje načina in opcij prikaza ter sprotna analiza pri zajemanju)

2.2 Filtri

S filtri se omeji in izloči za uporabnika zanimiv promet. Wireshark ima vgrajeno močno podporo za filtriranje prometa. Filterski parametri se vpisujejo v za to namenjena polja, v odvisnosti od vrste filtra. Vsi filtri delujejo tudi v realnem času (med zajemanjem prometa).

Wireshark loči dva tipa filtrov:

- zajemalne filtre – uporabijo se za filtriranje prometa v postopku zajemanja. Na ta način je mogoče določiti zanimiv promet ter omejiti količino zajetih podatkovnih enot in s tem

razbremeniti zajemalni terminal. Zajemalni filtri neposredno vplivajo na zajeti promet in ga omejujejo.

- prikazne filtre – uporabljajo se za omejevanje prikaza že zajetega prometa. Izmed celotnega nabora zajetih PDU se izloči samo zanimive, ki se prikažejo. Prikazni filter ne vpliva na zajeti promet temveč samo na njegov prikaz.

Primeri enostavnih prikaznih filtrov:

- selekcija po protokolu: v polje orodne vrstice filtra vpišemo ime protokola

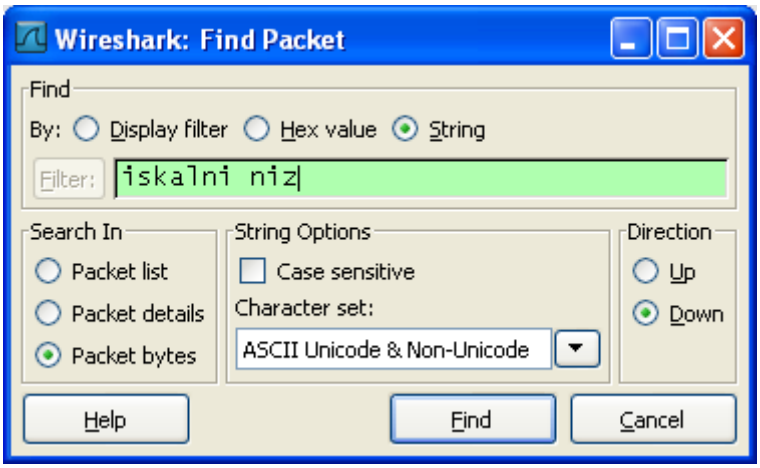
  `RTP, HTTP, ARP, TCP, UDP`

- selekcija po naslovu:

  `ip.addr eq 10.0.3.130`

- kombiniranje pogojev s pomočjo logičnih operatorjev `AND, OR, NOT`.

Wireshark omogoča iskanje znakovnih nizov, vsebovanih v podatkovnih enotah. Opcija glavnega menija Edit, Find Packet, omogoča podajanje iskalnega niza ter ostalih parametrov (slika št. 3).

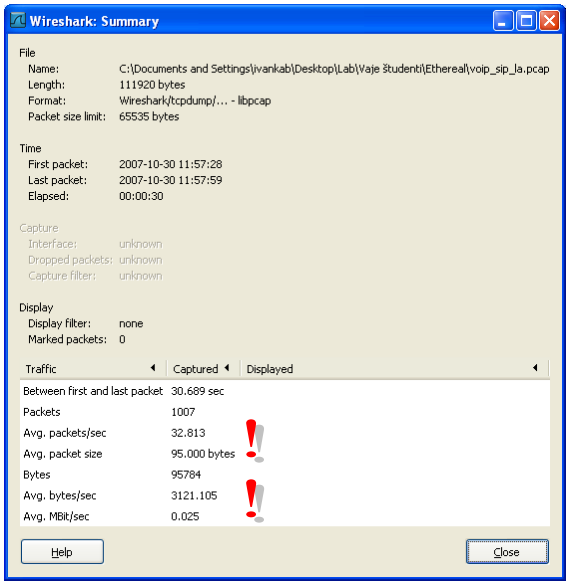


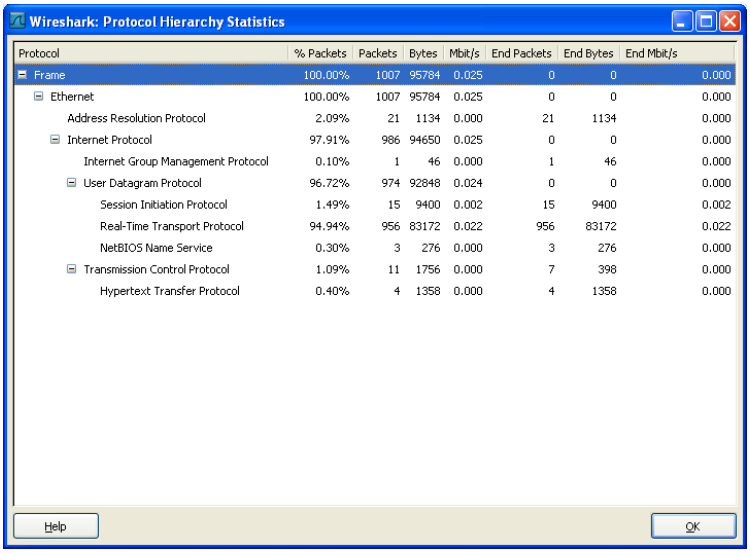
Sl. 3: Iskanje po vsebini zajetega prometa

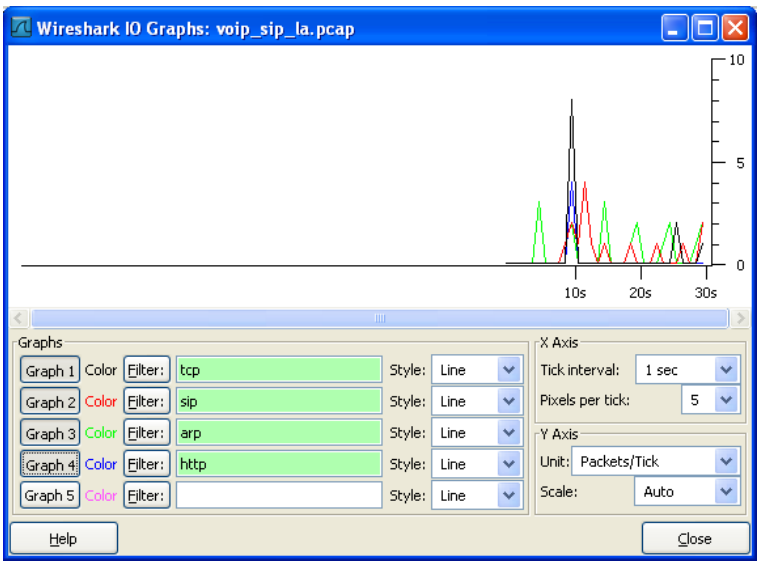
2.3 Statistična obdelava

Wireshark ponuja več orodij za statistično analizo prometa. Dostopna so v izbirniku **Statistics**. Zanimiva so:

- Summary – osnovne lastnosti zajetega prometa, kot so čas trajanja zajema, povprečna velikost podatkovnih enot, povprečna zahtevana pasovna širina;
- Protocol Hierarhy – podaja hierarhični vpogled v strukturo protokolov, prisotnih v zajetem prometu;
- Conversations – prikaz vzpostavljenih sej, oz. "pogovorjih" in
- Wireshark IO Graphs – orodje za grafično prikazovanje prometa.



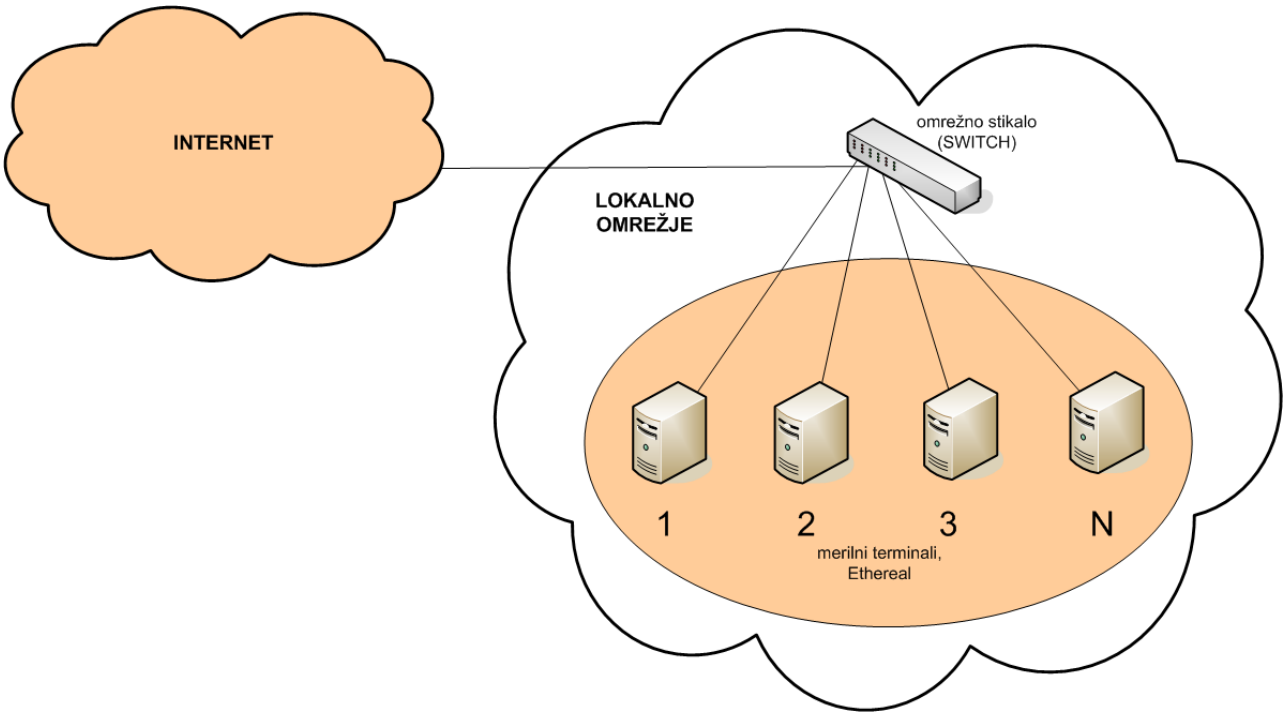




Sl. 4: Rezultati statistične analize /Summary, Protocol Hierarchy, IO Graphs)

3 NAVODILA ZA IZVAJANJE VAJE

3.1 Arhitektura merilnega omrežja



Sl. 5: Topologija merilnega omrežja

Pri vaji so uporabljeni naslednji elementi:

- osebni računalnik kot terminalna oprema,
- aplikacija Wireshark,
- omrežno stikalo (ang. switch).

Vsi merilni terminali so priključeni na omrežno stikalo. Ves zajem, meritve in analiza prometa poteka z uporabo orodja Wireshark.

Oglejte si arhitekturo merilnega omrežja in izpolnite nalogo 1 v poročilu.

3.2 Zaženite program Wireshark in si oglejte grafični vmesnik

3.3 Zajem splošnega prometa

Opravili bomo prvi zajem prometa. Pri zajemanju **ne uporabljajte** nobenih drugih aplikacij. Parametri zajemanja so naslednji:

- trajanje zajemanja: cca. *10 s*.

Oglejte si strukturo zajetega prometa in z uporabo funkcij statistične analize, ki so že vgrajene v orodje Wireshark:

- **izbirnik *Statistics->Summary*),**
- **izbirnik *Statistics->Protocol Hierarchy Statistics.***

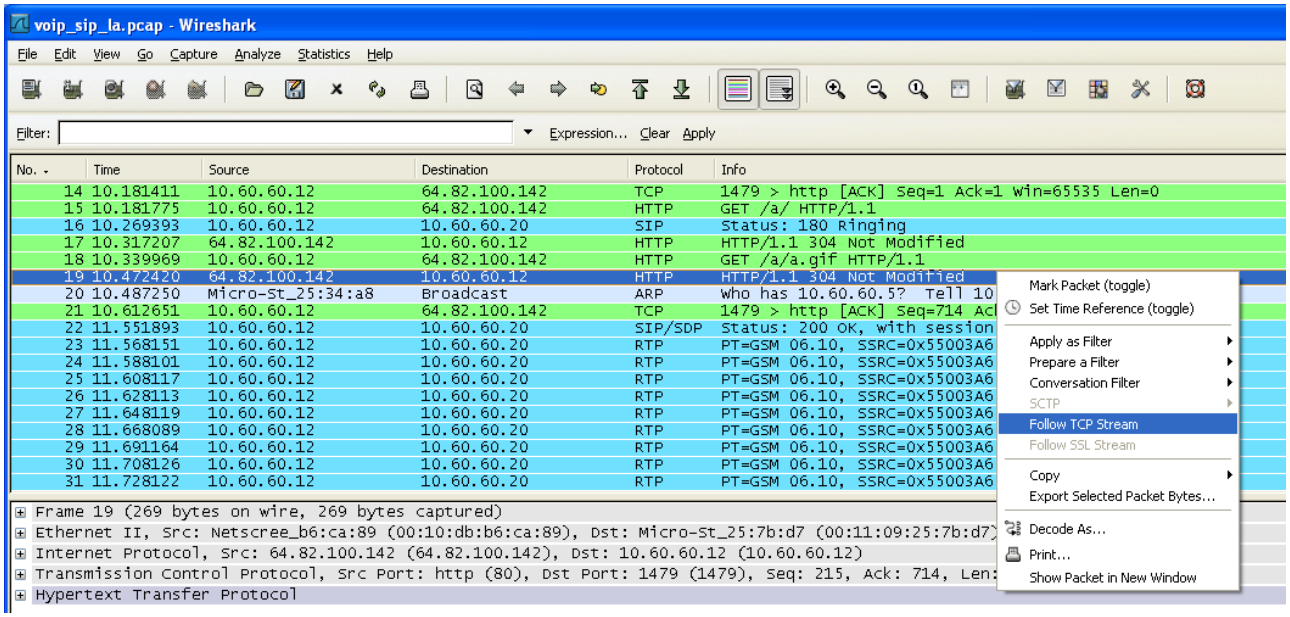
Izpolnite nalogo 2 v poročilu.

3.4 Zajem in filtriranje HTTP prometa

a. Sprožimo zajemanje prometa v navadnem načinu. Odprite spletni brskalnik in naložite poljubno spletno stran (npr. http://www.ltfe.org/, http://www.google.com). Končajte z zajemanjem prometa in zaprite brskalnik.

Izpolnite naloge 3.1.-3.3. v poročilu.

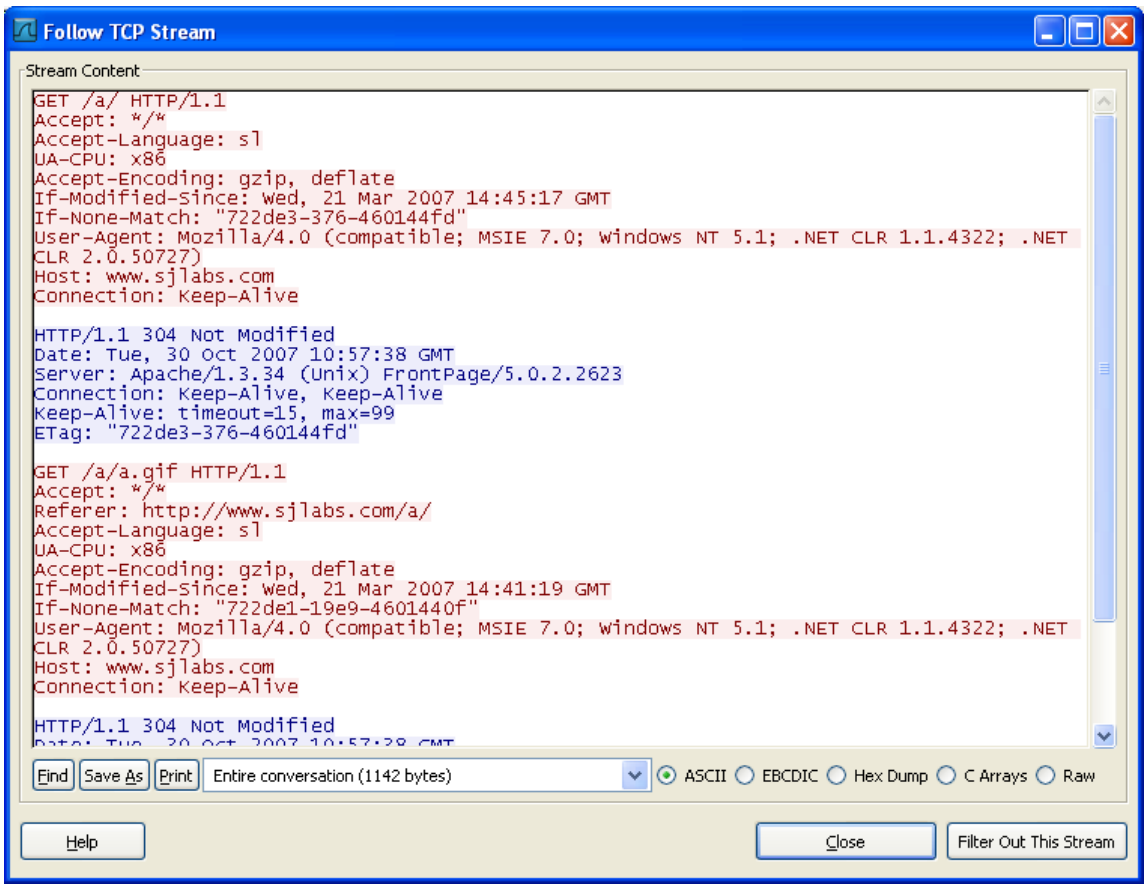
Izberite en HTTP paket iz zajetih paketov. Iz izbirnika, ki ga aktivirate s klikom na desno tipko miške, izberite opcijo **"follow TCP stream"**.



Sl. 6: Sledenje toku sporočil

S tem boste izločili samo tisti promet, ki je neposredno odgovoren za prenos določene spletne vsebine, ki ste jo obiskali. Izločijo se le sporočila, ki so logično povezana s pretokom podatkov po izbranem protokolu (HTTP) v okviru ene seje. Generira se tudi dekodiran prikaz prenešene informacije (npr. koda in vsebina spletne strani, slike, teksta, ...). Primer zasledenega prometa je podan na naslednji sliki.

Raziščite vsebino novoodprtega okna. Potem odgovorite na vprašanje 3.4. v poročilu.



Sl. 7: Dekodirana informacija (spletna stran)

b. Spet sprožimo zajemanje prometa v navadnem načinu. Tokrat s spletnim brskalnikom odpremo stran, ki zahteva uporabniško interakcijo (vnos podatkov za nadaljevanje). To je lahko kakšen iskalnik (google, najdi.si) ali spletna enciklopedija (Wikipedia) ali spletni poštni portal (e-mail). V namene vaje ne uporabljajte stran, ki zahteva vnos osebnih podatkov, uporabniških imen ali gesel. Po vnosu in oddaji podatkov, prekinite zajemanje. Potem odgovorite na vprašanje 3.5, 3.6. v poročilu.

3.5 Zajemanje in filtriranje video prometa

Video promet simuliramo z uporabo video odjemalca, ki omogoča predvajanje videa v realnem času. Izbrani odjemalec je MS Windows Media Player.

V Wireshark-u sprožimo zajemanje prometa v navadnem načinu. V MS Media Playerju sprožimo predvajanje video vsebine – v izbirniku *File → Open URL* vpišemo naslov video vira:

```
rtsp://212.235.185.101/LTFEHosting/Zmagovalna2.wmv
rtsp://212.235.185.101/LTFEHosting/Zmagovalna1.wmv
```

Ustavimo video tok. Končamo zajemanje. Po končanem zajemu je razvidna tipična kombinacija protokolov, ki se uporabljajo za prenos večpredstavnih vsebin v realnem času (npr. RTSP/RTP). Izpolnite točko 4 v poročilu.

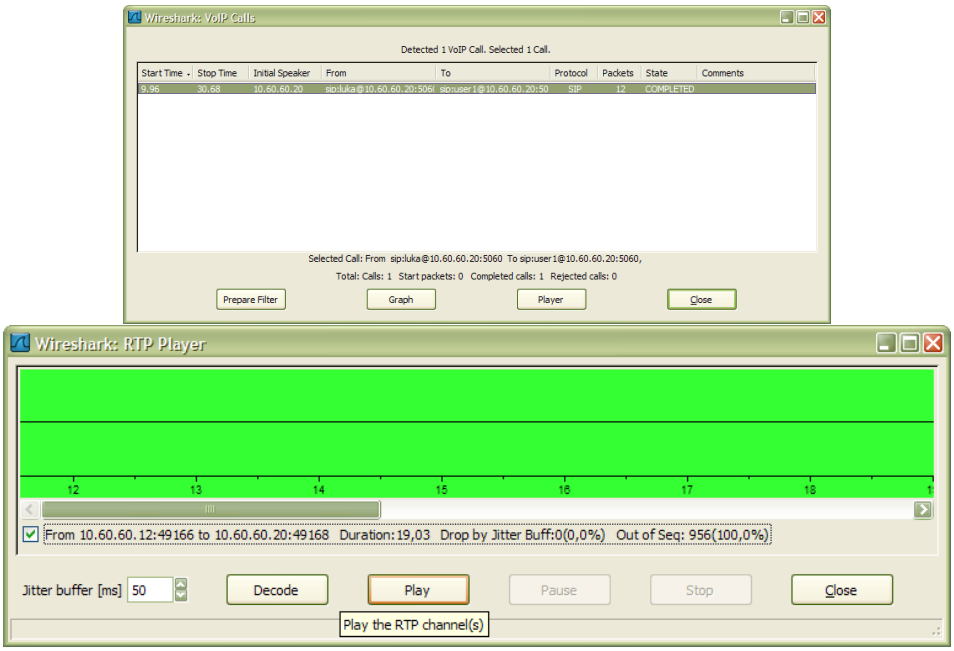
Poskusite zajeti tudi promet pri prenosu video vsebin s spletnih video portalov (npr. Youtube, mojvideo.com, www.sitv.tv) .

3.6 Demo: zajemanje in filtriranje VoIP prometa

Sprožimo zajem podatkov. Na VoIP klientu (SJPhone) izvedemo klic na drugi klient. Ustavimo zajemanje. Zajeta struktura sporočil odraža tipično kombinacijo protokolov za prenos zvoka v realnem času pri telefoniji IP.

Z obdelavo vsebine zajetega prometa je možno dekodiranje zvočnega signala telefonskega pogovora. Če komunikacija ni dodatno zaščitena je to lahko primer potencialne zlorabe oz. prisluškovanja pri telefoniji IP.

V izbirniku izberemo *Telephony → VoIP Calls*. Na zaslonu se pojavi seznam VoIP klicev, ki so prisotni v zajetem prometu. Na sliki je prikazan izgled zaslona.



Sl. 8: Dekodiranje zvočne vsebine iz prometnega toka

Izberemo želeni klic in s klikom na gumb Play zaženemo dekodiranje zvočne vsebine. Wireshark omogoča takojšnje predvajanje dekodirane vsebine.