L1.2 Wireshark

Cilji vaje

> - Spoznati orodje Wireshark.
> - Analiza vnaprej zajetega ("posnetega") prometa iz datoteke formata .cap ali .pcap.
> - Zajemanje prometa "v živo".

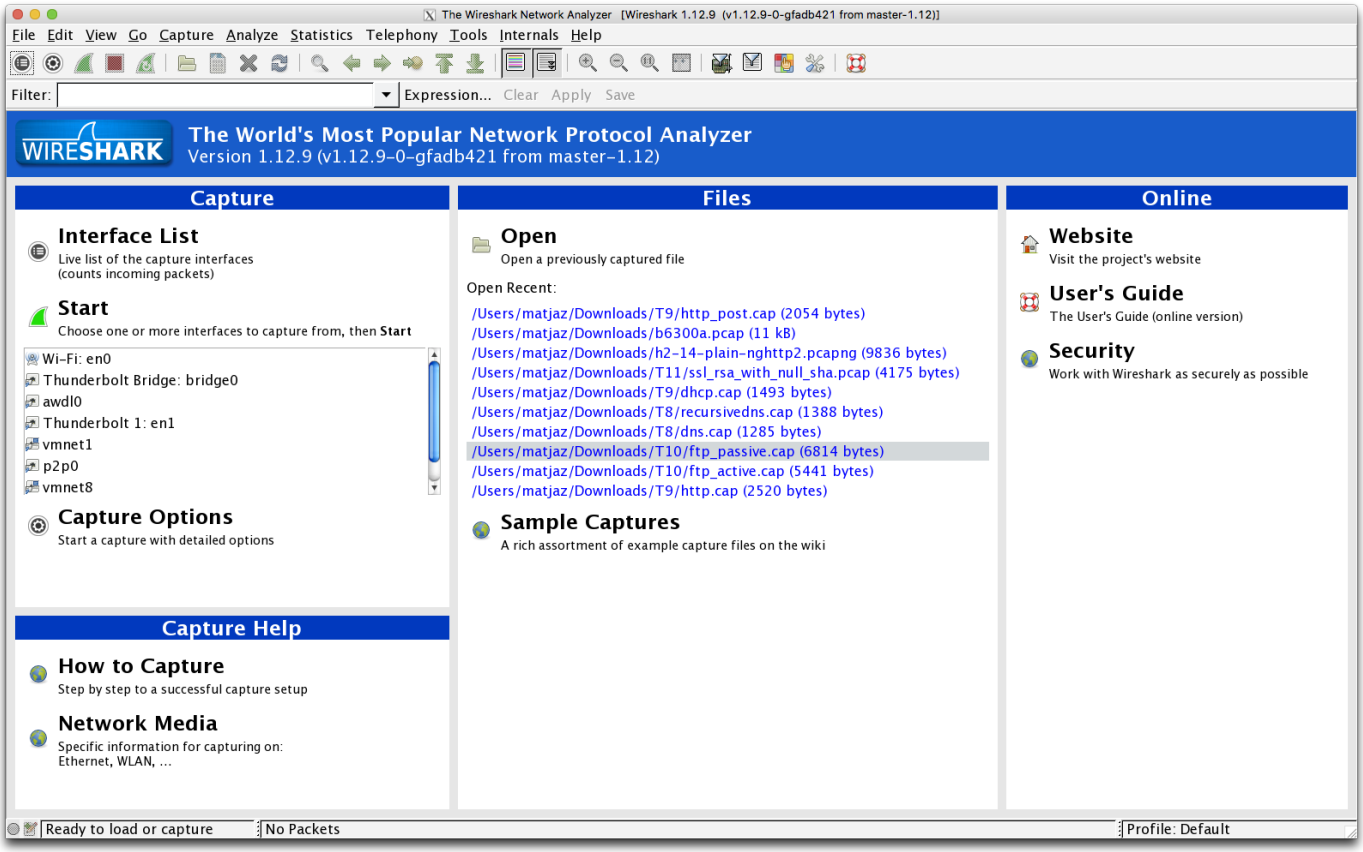
Wireshark je najbolj razširjeni grafični pregledovalnik in snemalnik omrežnega prometa, s katerim lahko delamo tudi kompleksna filtriranja, analize in statistike na omrežnem prometu. Podpira praktično vse znane (in manj znane) omrežne protokole.

Pri Računalniških komunikacijah ga bomo zelo pogosto uporabljali za analizo protokolov, o katerih se bomo učili pri predmetu.

Wireshark - kratka navodila za uporabo

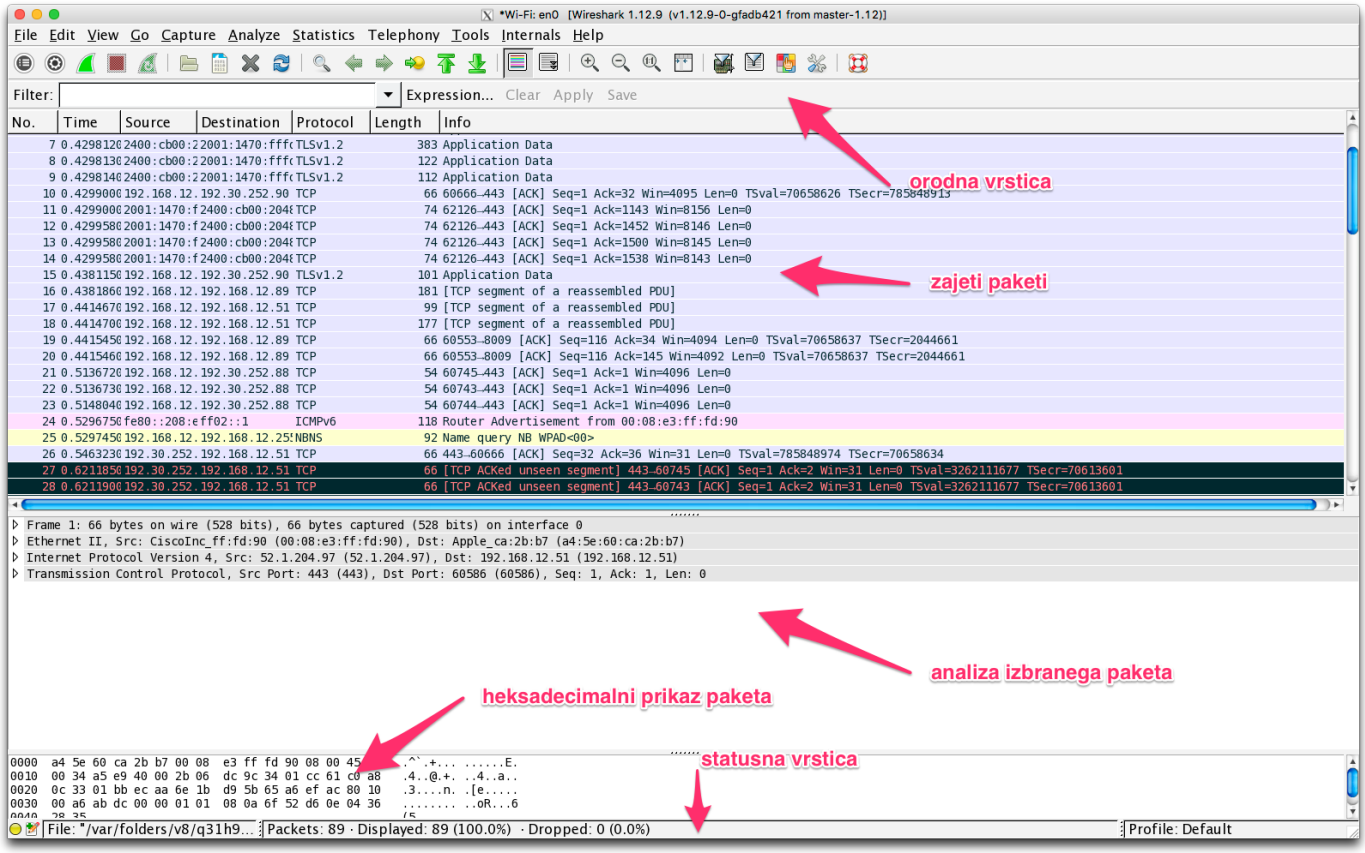
> Ker je bila računalniška učilnica, v kateri pravkar sedite, pripravljena že jeseni, ne bomo uporabljali najnovejše verzije Wiresharka (v2.x), ampak starejšo različico v1.12. Ko si boste doma instalirali Wireshark, si lahko brez problemov namestite najnovejšo različico, saj je funkcionalno enaka, le da ima malo spremenjen in izboljšan uporabniški vmesnik.

Ko Wireshark zaženete, se prikaže začetno okno:



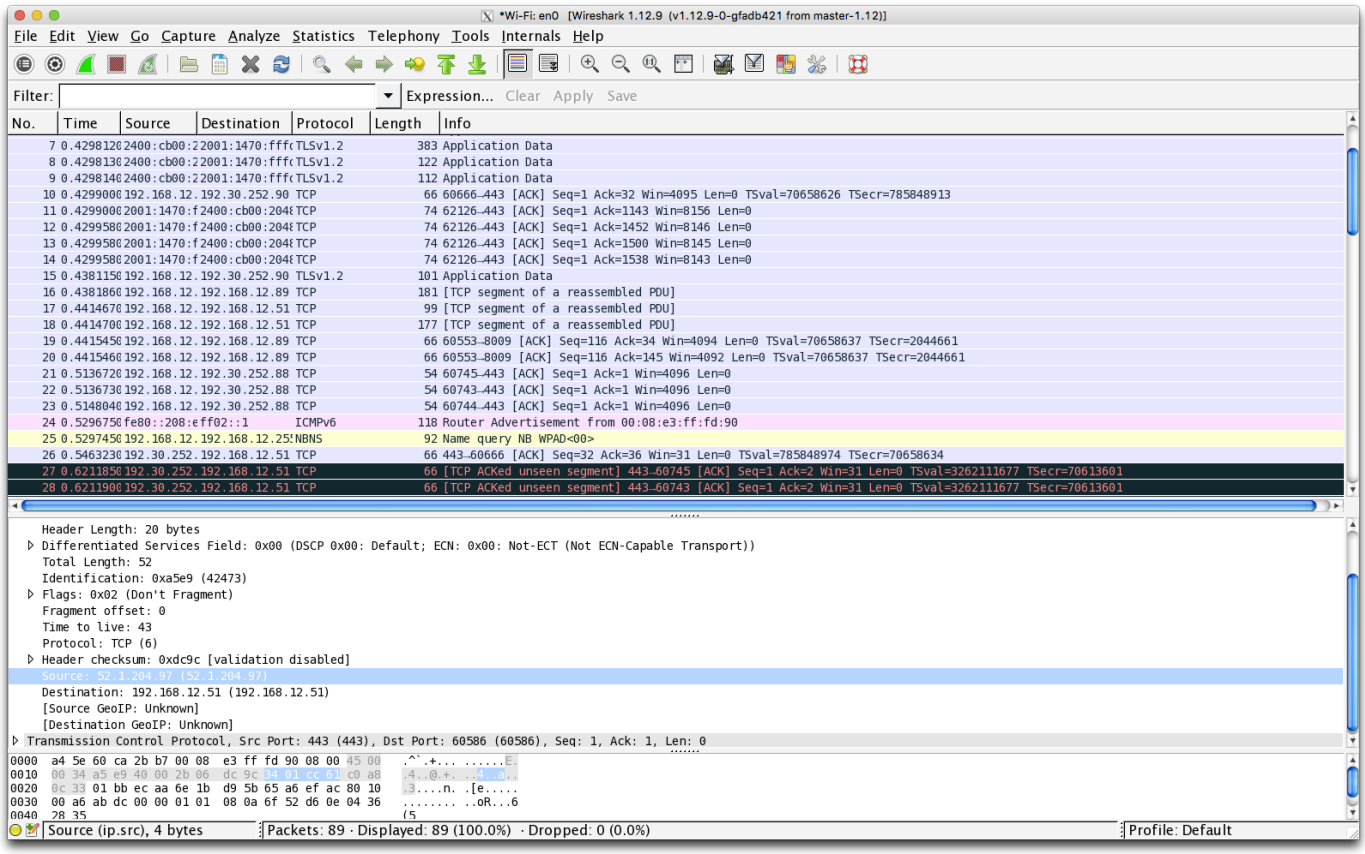
V *Capture* oknu vidite vaše omrežne adapterje in lahko kar takoj začnete zajemati ("snemati") promet. V *Files* vam pokaže zgodovino odprtih datotek s prometom, V *Help* in *Online* pa imate povezave na pomoč.

Ko odprete (*File/Open*) kakšno datoteko s prometom *.pcap (packet capture)*, se vam odpre naslednje okno:

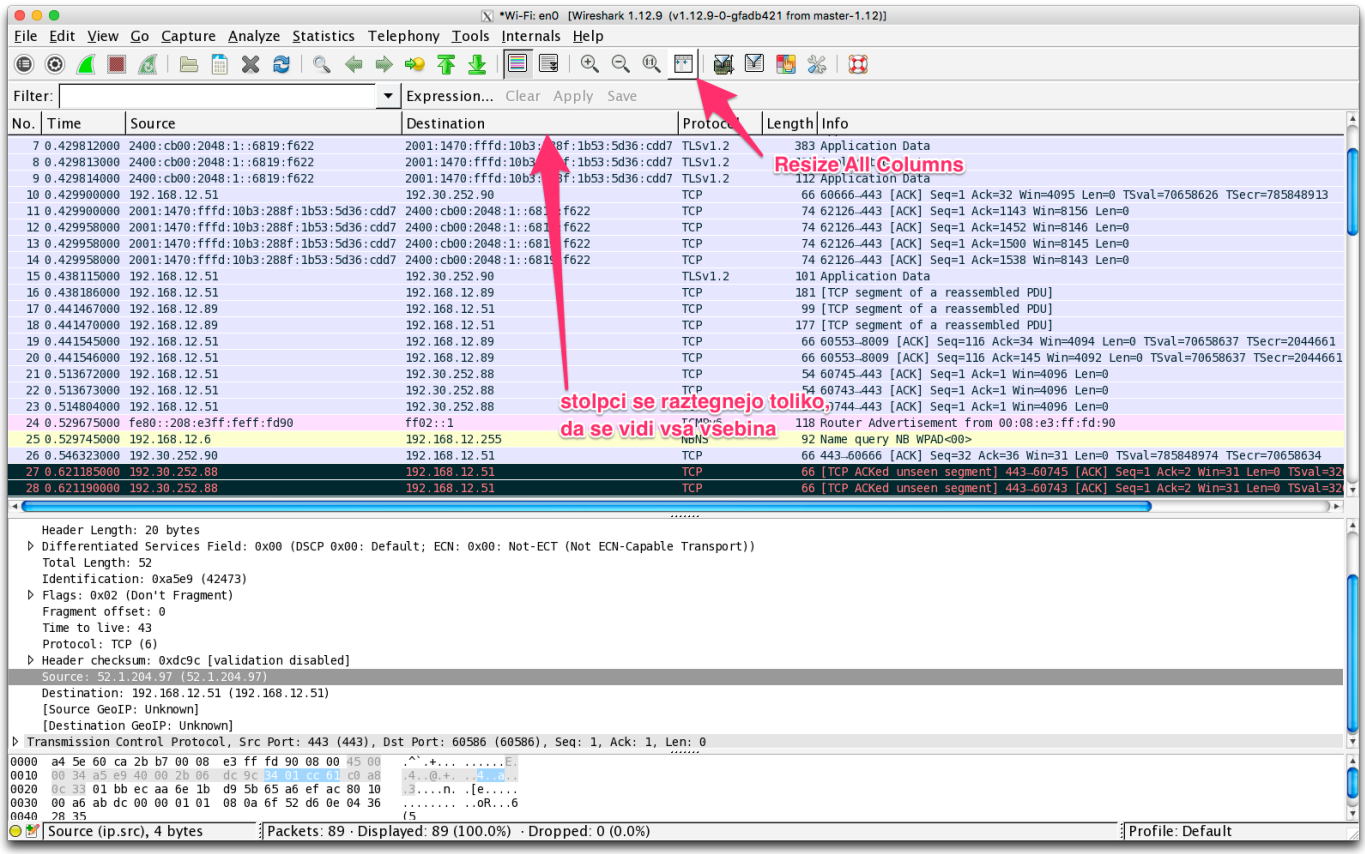


1. Čisto na vrhu je orodna vrstica z menujem.
2. Sledi osrednje okno, kjer vidite posamezne pakete, po enega v vsaki vrstici. Vrstice vam Wirehark obarva glede na protokole in morebitne napake v paketu (črno so recimo podvojeni paketi, itd.). Vrstica je razdeljena na več stolpcev:
   - No.: zaporedna številka paketa
   - Time: časovni zamik prispetja paketa v sekundah (glede na prvi paket)
   - Source: pošiljatelj paketa
   - Destination: prejemnik paketa
   - Protocol: protokol, ki je v paketu, tu napišemo tistega, ki je najvišje glede na plasti (torej najbližje aplikacijski plasti)
   - Length: dolžina v bajtih
   - Info: polje, v katerem vam Wireshark prikaže najpomembnejše informacije v kontekstu protokola, ki je v paketu (različni protokoli imajo različne poudarke glede tega, kateri podatki se običajno veliko uporabljajo). V vsakem primeru so vsi ti podatki prisotni tudi v podrobni analizi paketa v oknu pod spiskom paketov.
3. Sledi okno z analizo izbranega paketa. Če v zgornjem oknu izberete (kliknete) na posamezen paket, vam v tem oknu Wireshark naredi podrobno protokolarno analizo.
4. Pod protokolarno analizo sledi okno, kjer imate zajeti paket prikazan takšen, kot se pošilja "po žicah", levo v heksadecimalnem zapisu, desno, v zadnjih dveh stolpcih, pa vam vsak byte posebej še izpiše kot znak ASCII kodne tabele.
5. spodaj je statusna vrstica

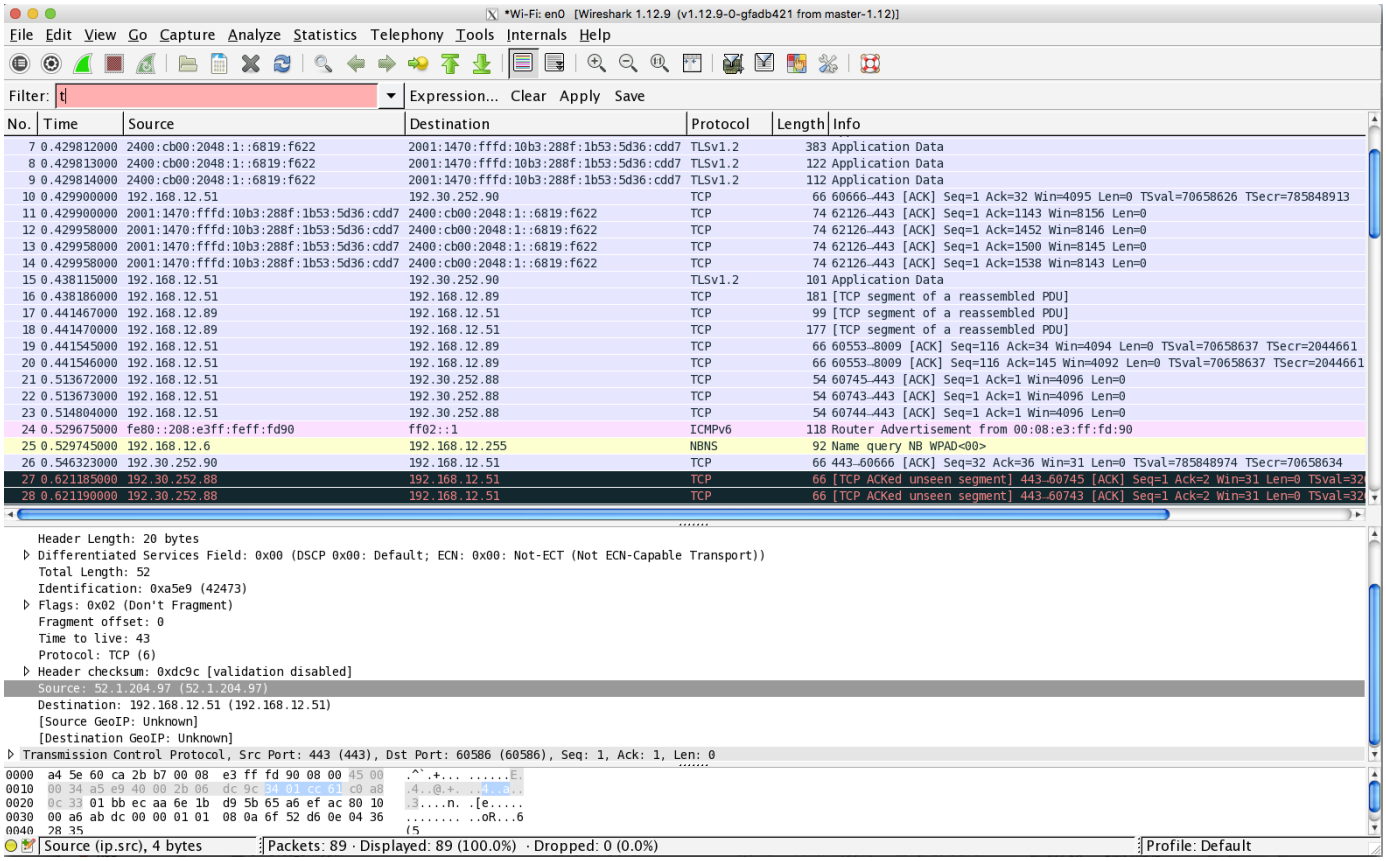
Če v oknu analize prokotola kliknete na posamezni protokol (enojni klik levo na trikotnik pred vrstico ali dvojni klik na vrstico), se vam odpre podrobna analiza posameznega protokola. Slika spodaj recimo prikazuje izpis, ki se naredi, če kliknete na tretjo vrstico *Inetnet Protocol Version 4*.



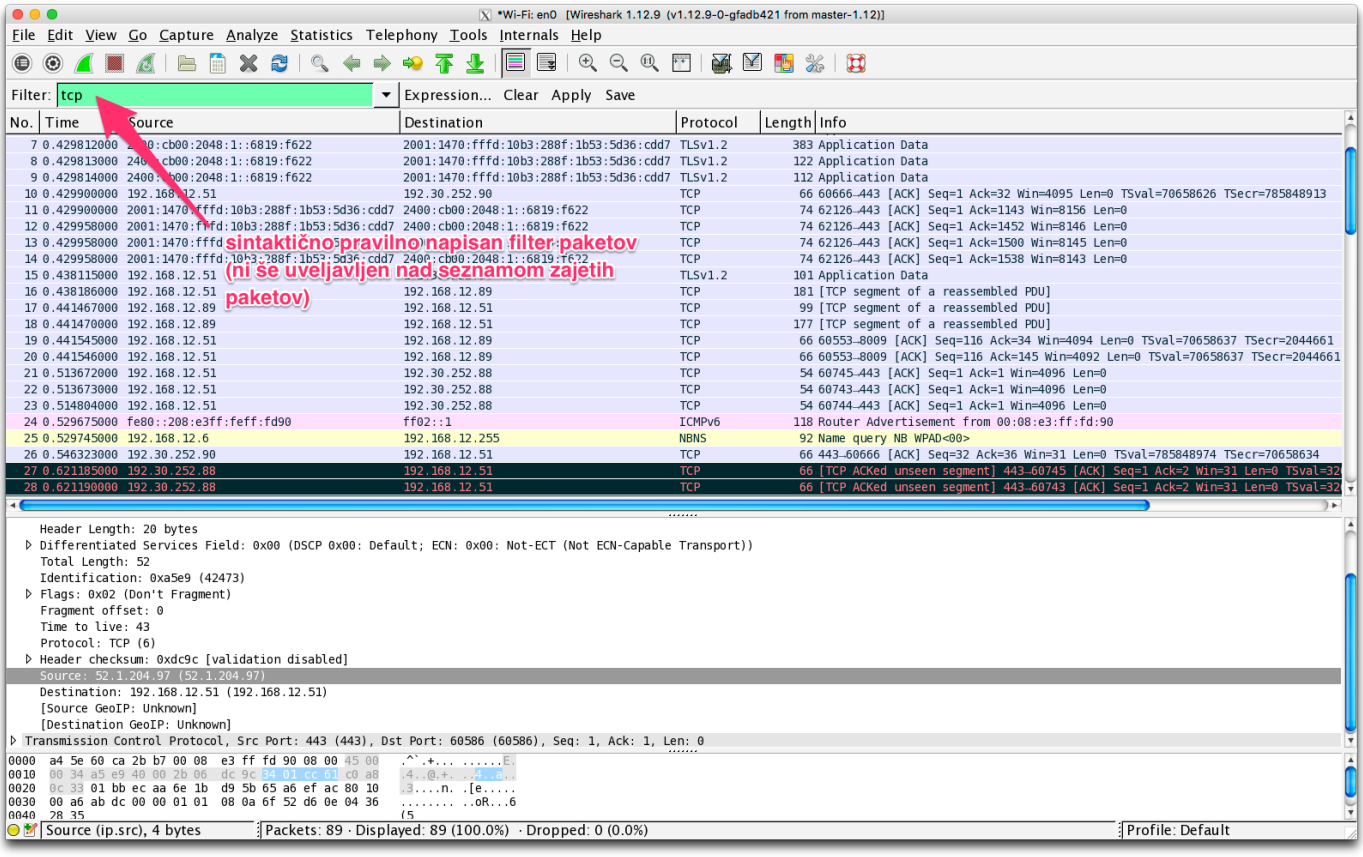
V spisku paketov (osrednje okno) včasih ne boste videli vsebine celotnega stolpca. Če želite videti vse, lahk kliknete na gumb v orodni vrstici *"Resize All Columns"*:



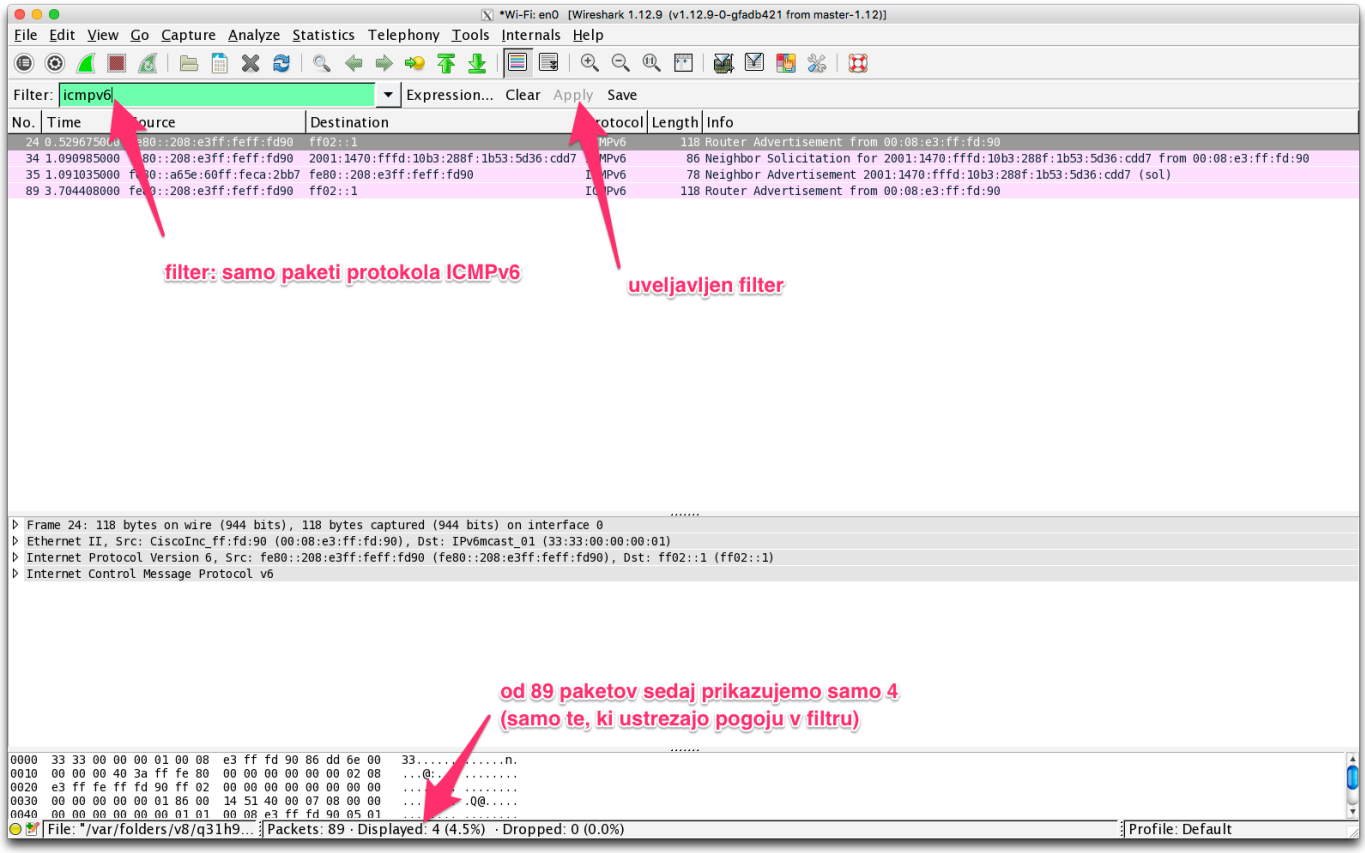
Opazili boste, da je v večini primerov za analizo potrebno iz spiska vseh paketov prikazati samo določene pakete. To storite v okenčku orodne vrstice *"Filter"*. Filtri so lahko zelo kompleksni (uporabljate lahko tudi Boolovo algebro). Najenostavnejše je filtriranje po posameznem protokolu (torej hočemo prikazati samo pakete, ki vsebujejo določen protokol, ostali paketi, ki vsebujejo druge protokole, pa nas ne zanimajo).



Wireshark vam pomaga pri pisanju filtra: dokler je okence rdeče, filter ni sintaktično pravilen. Ko je okence zeleno, je filter sintaktično pravilen.



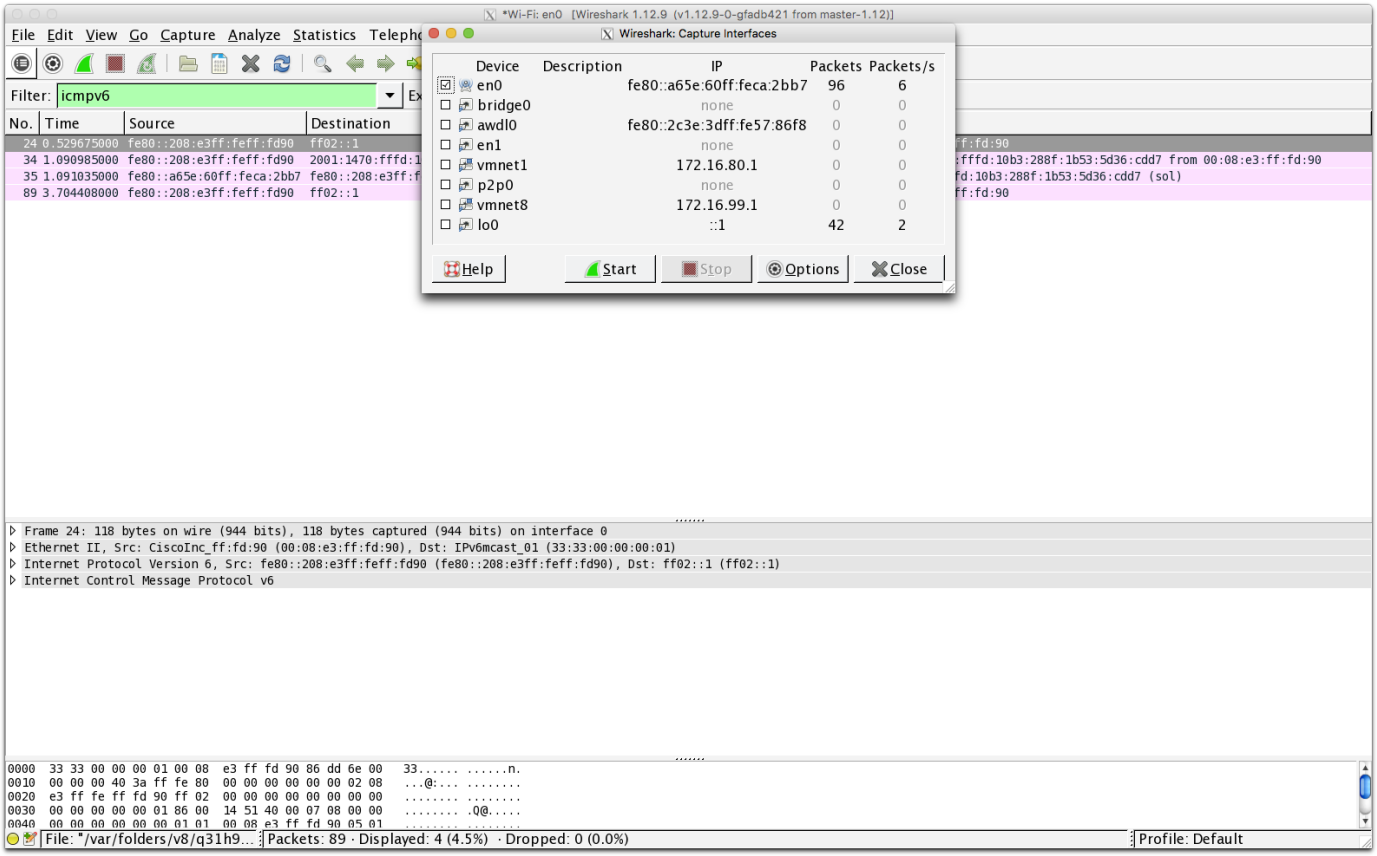
Sintaktično pravilne filtre lahko uporabite na seznamu paketov (kliknete *"Apply"* ali pritisnite enter ko je kurzor v okencu filtra):



Pozorni bodite na to, da filtriranje pakete ne izbriše iz seznama, ampak jih samo ne prikaže. Še vedno v statusni vrstici vidite, da vsebuje datoteka ravno toliko paketpov, kot pred uveljavitvijo filtra.

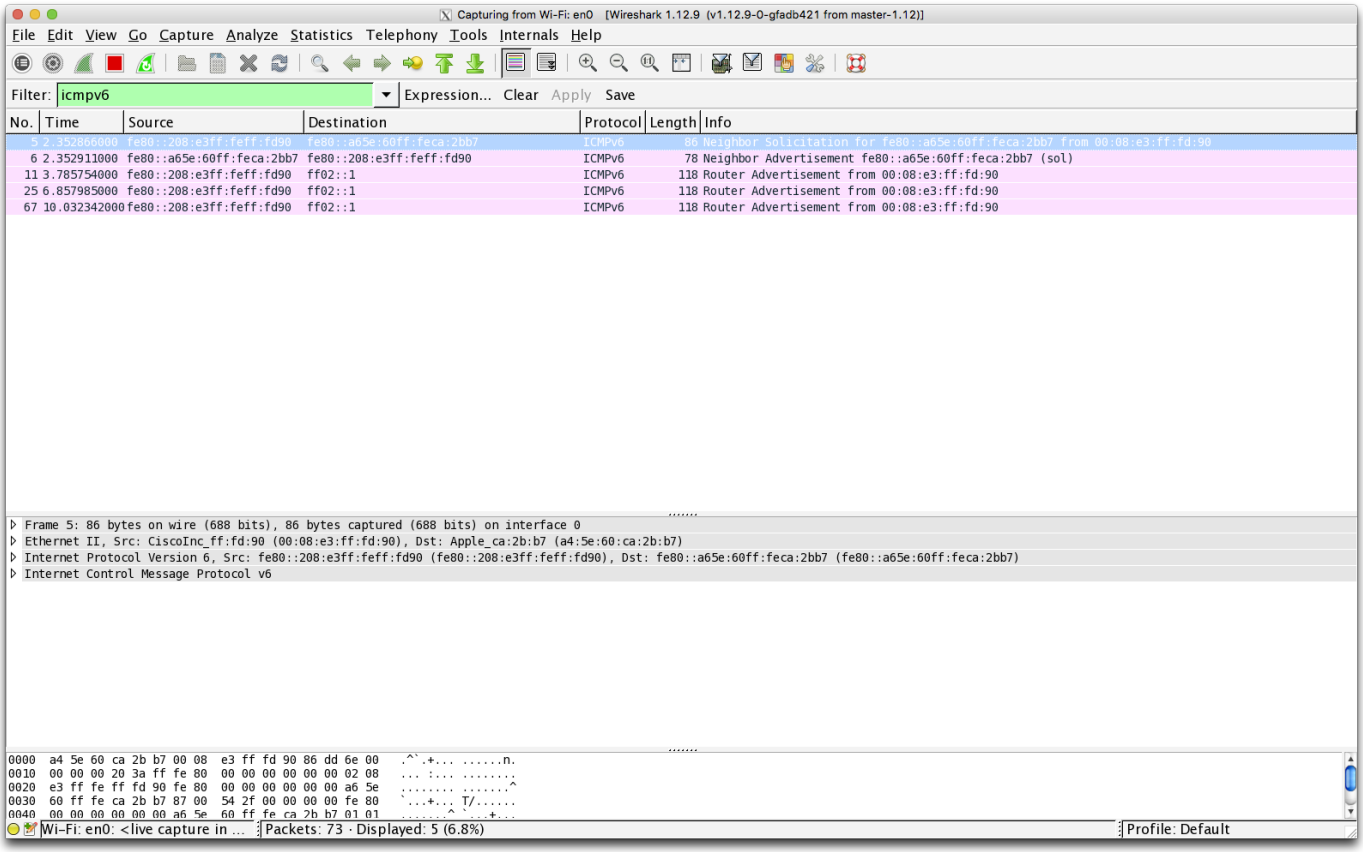
Zajemanje prometa "v živo"

Včasih želimo promet spremljati v živo, torej da Wireshark takoj, ko kakšen paket pride do nas, le tega prikaže v seznamu. V tem primeru moramo sprožiti zajem paketov na enem izmed vmesnikov, ki je dostopen na računalniku. Če kliknete prvo ikono (*"Capture interfaces"*), dobite seznam vseh vmesnikov, ki jih vidi vaš operacijski sistem. Bodite pozorni na to, da različni operacisjki sistemi različno označujejo omrežne vmesnike (Linux kot eth, Mac kot en, Windows spet z dolgim logičnim imenom. Če imate na računalniku še kakšen virtualizacijski program (VirtualBox, VMware, ...), je teh adapterjev z eksotičnimi imeni še mnogo več. Slika prikazuje adapterje na prenosniku z OS X (Mac):



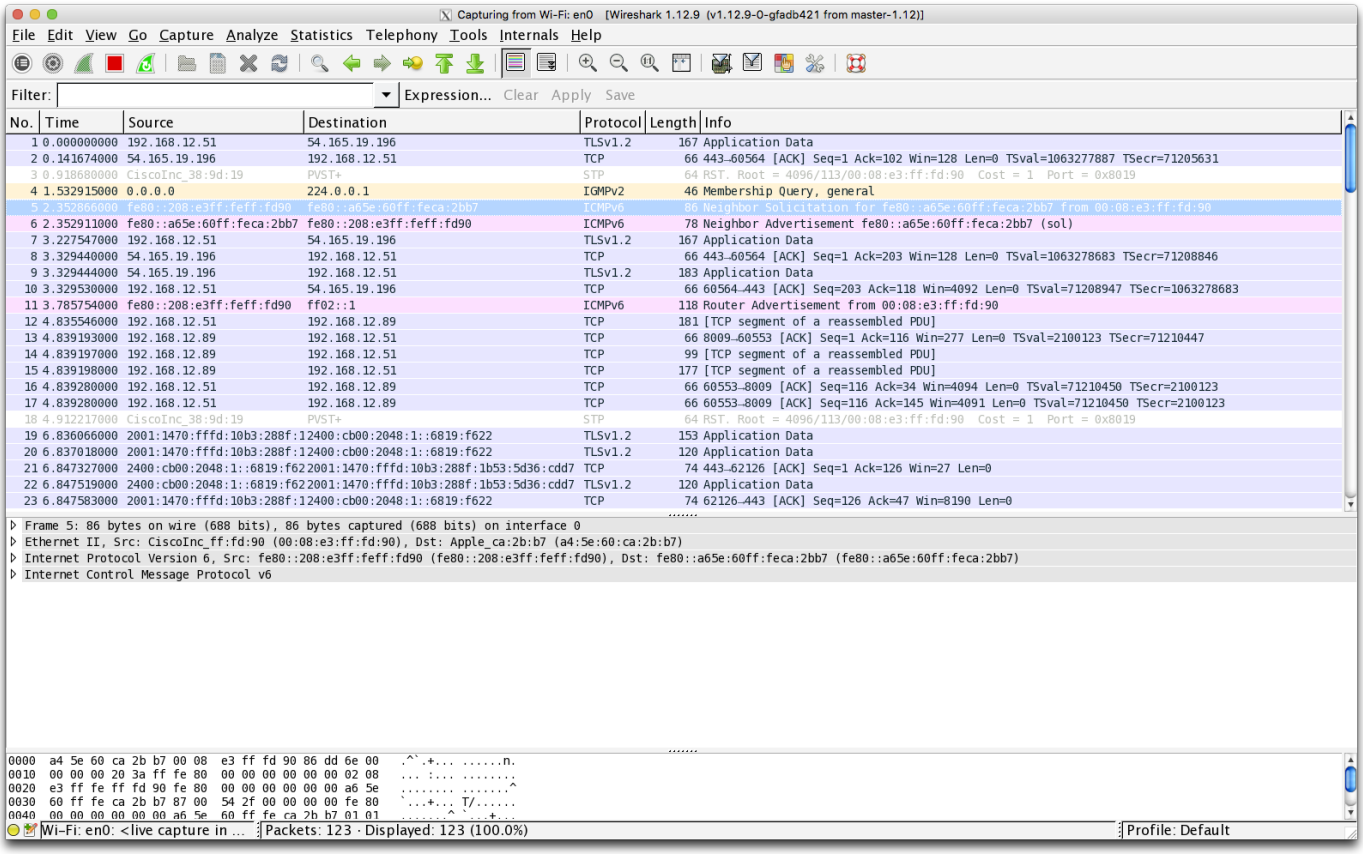
Vmesnik, ki prejema po statistika največ prometa, je ponavadi tisti "glavni", preko katerega običajno zajemamo promet. Lahko pa sprožite tudi zajem preko **vseh** možnih vmesnikov, ki so dostopni temu računalniku in so vklopljeni.

Zajemimo promet v živo (klik na tretjo ikono *"Start a new live capture"*). Sedaj vidite v živo, kako se posamezni prispeli in oddani paketi dodajajo v seznam. Ker imamo tu tudi aktiviran Filter ("icmpv6"), potem nam sicer v ozadju zajema vse pakete, prikaziuje pa samo te, ki ustrezajo filtru. To je zelo uporabna funkcija, ki so velikokrat uporabljamo pri odpravljanju omrežnih težav.

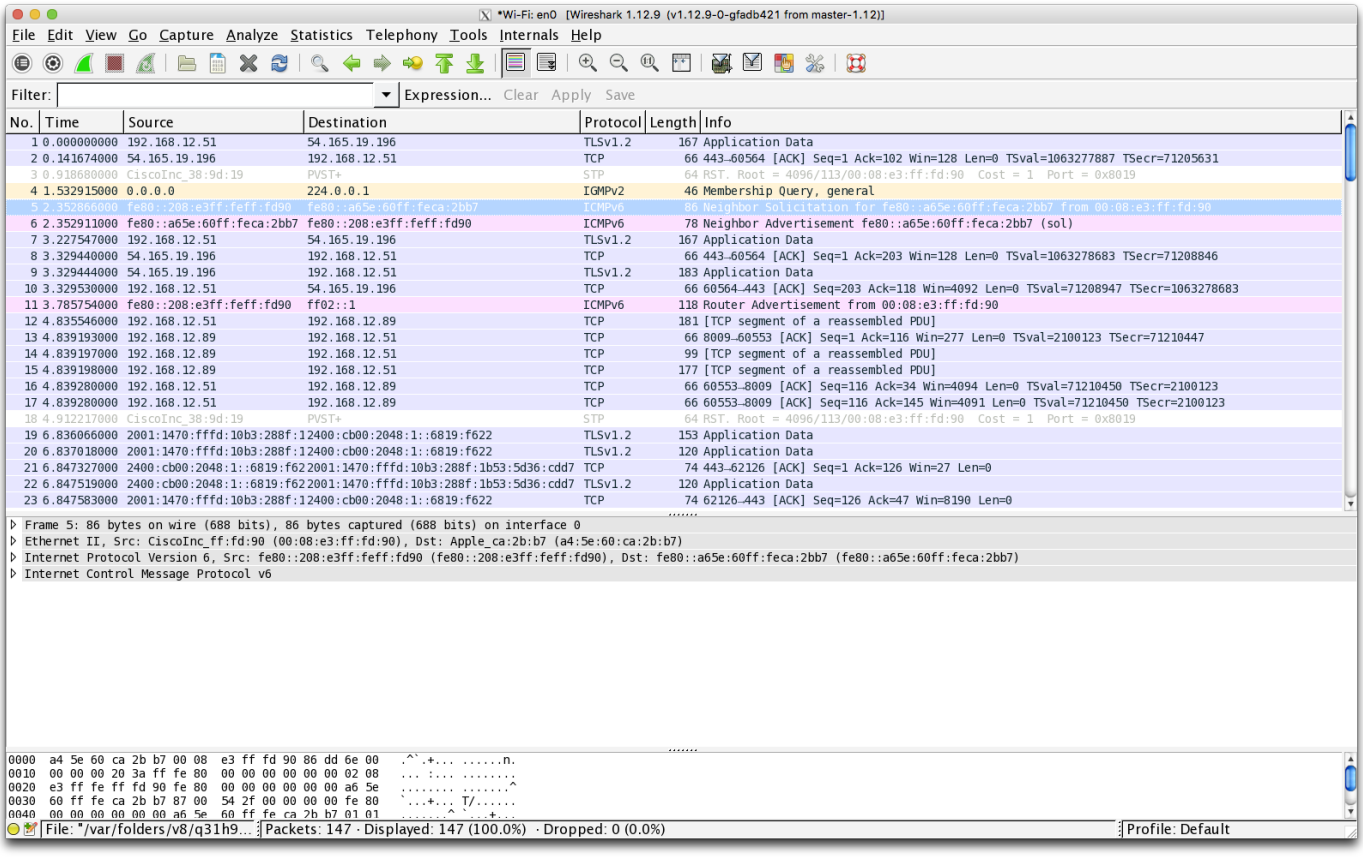


Če želite videti zajete pakete, potem kliknite na gumb *"Clear"* zraven okenca za filter. Wireshark vam sedaj prikaže vse pakete,

ki so bposlani ali sprejeti na izbranem omrežnem vmesniku.



Ko želite prekiniti zajemanje, kliknite na četrto ikono *"Stop the running live capture"*.



Sedaj lahko pakete, ki ste jih zajeli, tudi shranite v .pcap datoteko (*"File/Save ali SaveAs"*).

Naloge

S programom Wireshark odprite datoteko L1_3.cap. Preučite pakete in odgovorite na spodnja vprašanja:

1. Za kateri protokol gre pri prikazanih paketih?
2. Pri prikazanem protokolu vidimo, da se izmenjujeta 2 tipa sporočil. Za kateri sporočili gre?
3. Kdo je pošiljatelj paketa št. 1? Kdo pa prejemnik?
4. Kdo je pošiljatelj paketa št. 2? Kdo pa prejemnik?

V zgornjih nalogah ste uporabljali promet iz datoteke, ki smo jo za vas predhodno pripravili. V programu Wireshark sprožite zajem prometa in odgovorite na spodnja vprašanja:

1. Kakšen filter morate napisati, če želite videti samo pakete, ki jih pošilja in sprejema program ping?
2. Kakšne podatke pošilja program ping proti prejemniku? Kako dolg je posamezni paket (upoštevajte celotno dolžino paketa)?