CARNET

# Wireshark

NCERT-PUBDOC-2018-1-352

CERT.hr

# Sadržaj



Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# 1 Uvod

Računala se svakim danom sve više koriste za komunikaciju. Ta komunikacija se odvija preko računalnih mreža korištenjem brojnih mrežnih protokola. Zato je važno imati mogućnost pregleda i analize mrežnog prometa.

Wireshark je najpoznatiji alat za snimanje i analizu mrežnog prometa. On omogućava snimanje mrežnog prometa odabranog mrežnog sučelja te njegovo interaktivno pregledavanje i analizu. Wireshark prepoznaje više stotina protokola te ih u svom sučelju prikazuje u strukturiranom i čitljivom formatu. Prva inačica alata nastala je 1998. godine pod imenom Ethereal, no 2006. godine projekt mijenja ime u Wireshark. Wireshark je slobodan softver (eng. *free and open source*) te je dostupan na većem broju platformi, uključujući Microsoft Windows, Linux, macOS, Solaris i BSD.

Analiza mrežnog prometa vrlo je važna u radu IT stručnjaka. Neke od važnih primjena su:

- Pomoć pri razvoju mrežnih protokola
- Traženje pogrešaka u implementaciji mrežnih protokola
- Analiziranje ponašanja zloćudnih programa

Wireshark je također odličan alat za edukaciju i upoznavanje s osnovama rada računalnih mreža i protokola.

Kao i gotovo svi drugi alati, Wireshark je moguće koristiti i u zlonamjerne svrhe. U određenim situacijama, napadač pomoću Wireshark-a može prisluškivati mrežni promet žrtve te saznati njene povjerljive podatke ako promet nije šifriran. Najveći rizik od ovakvog prisluškivanja imaju bežične (npr. Wi-Fi) mreže.

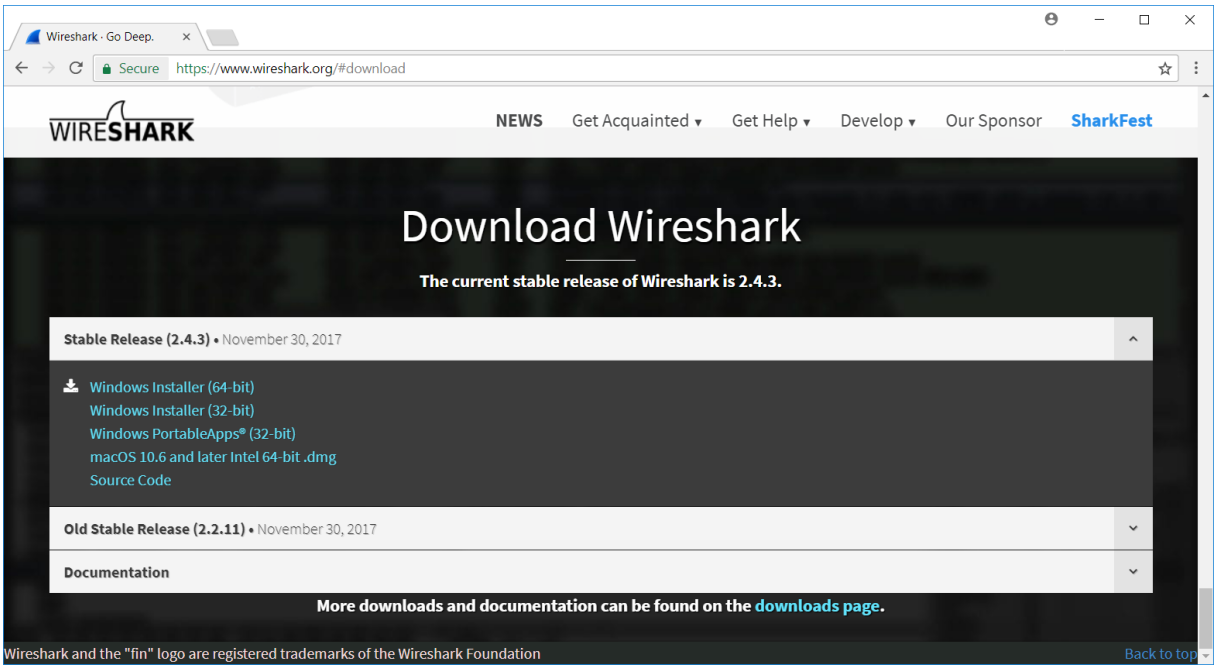
U ovom dokumentu bit će prikazan postupak instalacije alata Wireshark te jednostavni primjeri njegovog korištenja – osnovno filtriranje paketa te analiza DNS i HTTP prometa.

# 2 Instalacija i korištenje

## 2.1 Instalacija

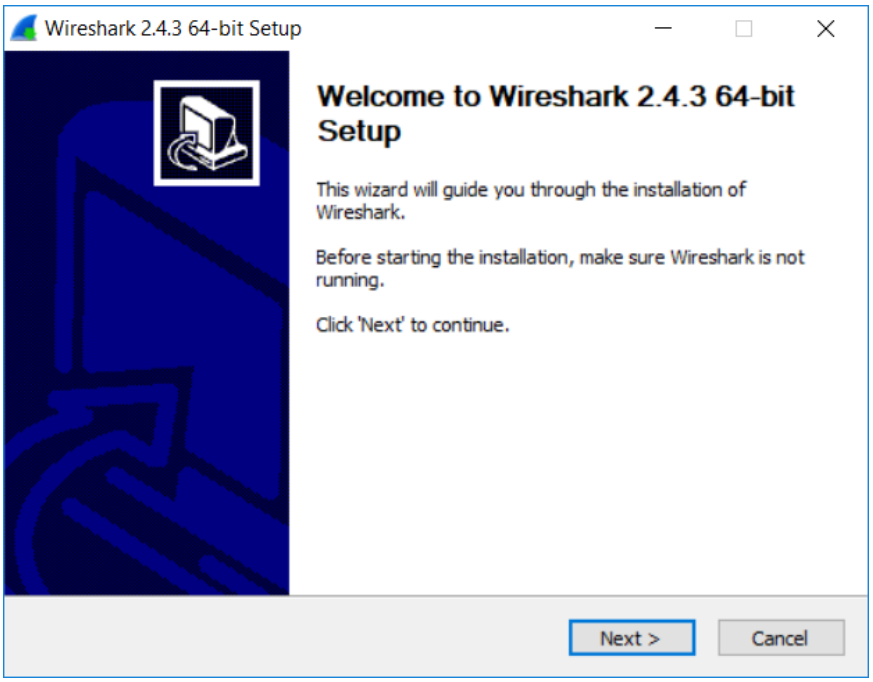
Postupak instalacije alata Wireshark bit će opisan za operacijski sustav Windows. Koraci za instalaciju su sljedeći:

1. Prvo je potrebno preuzeti odgovarajuću inačicu Wireshark-a s ove poveznice. U ovom primjeru to je „Windows Installer (64-bit)“.



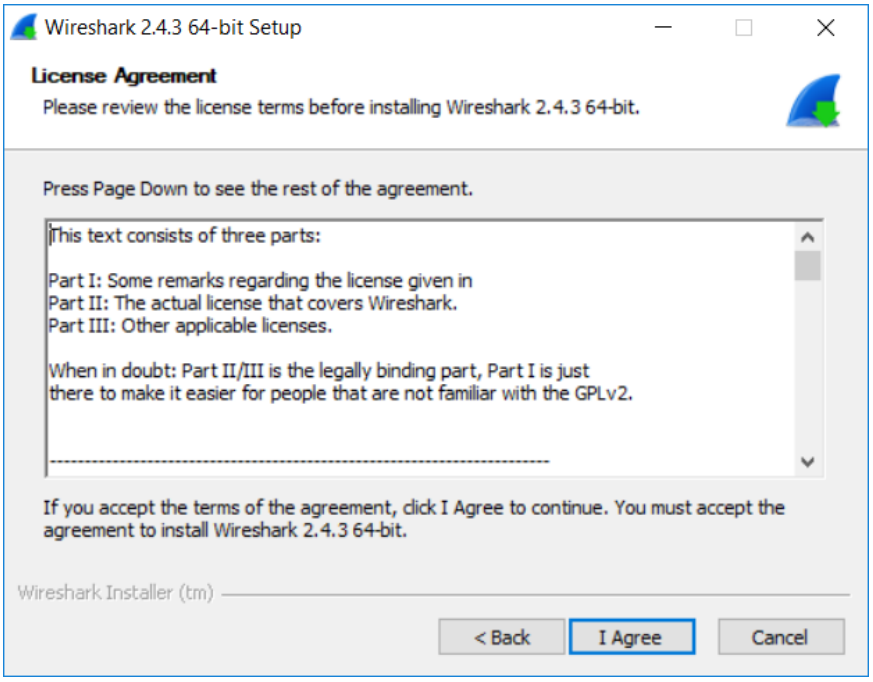

**Slika 1**

2. Nakon preuzimanja i pokretanja datoteke otvara se instalacijski prozor na engleskom jeziku. Potrebno je kliknuti na ***Next*** za sljedeći korak.



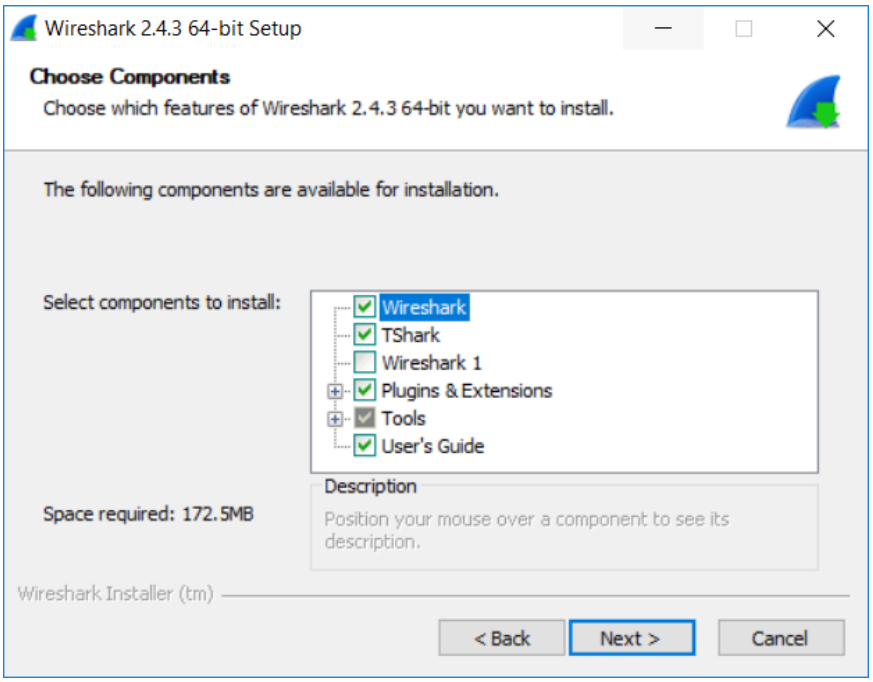

**Slika 2**

3. U sljedećem koraku potrebno je složiti se s uvjetima korištenja klikom na ***I agree***.



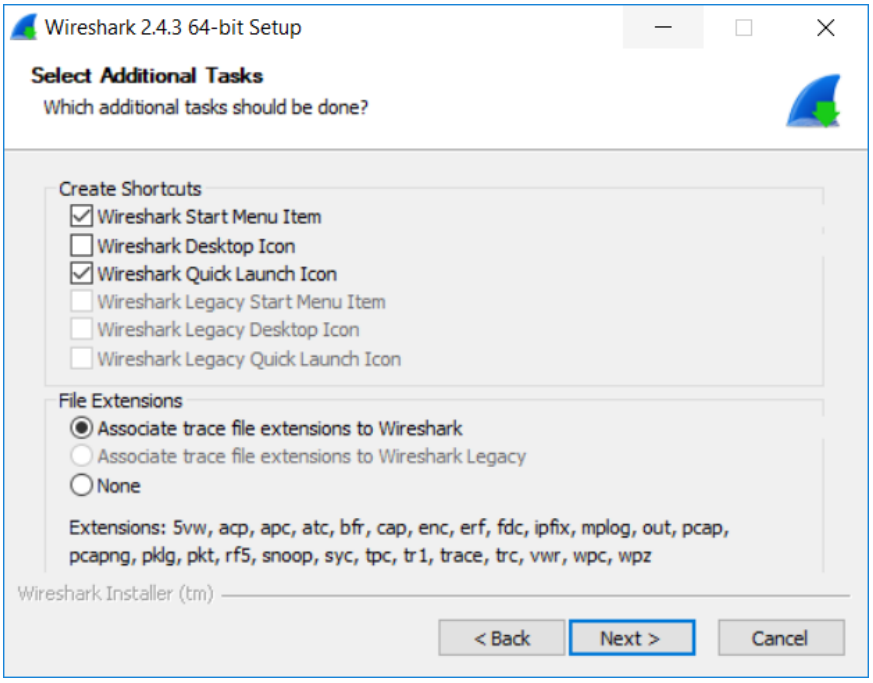

**Slika 3**

4. Potrebno je odabrati komponente koje će se instalirati kao što je prikazano na slici te kliknuti ***Next***.



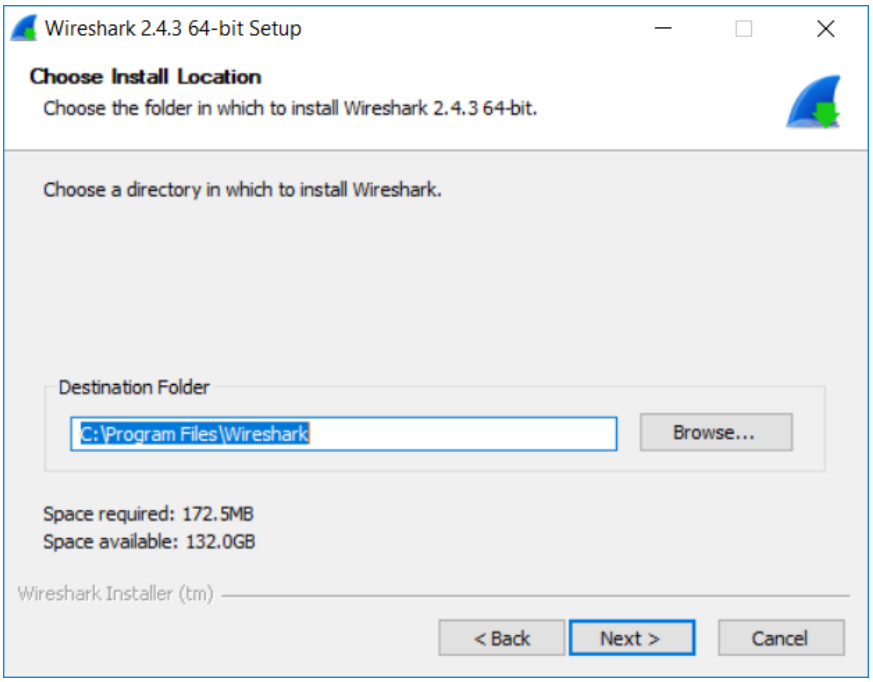

**Slika 4**

5. Zatim je potrebno odabrati gdje će u sustavu biti stvorene poveznice na Wireshark te kliknuti ***Next*** za sljedeći korak.



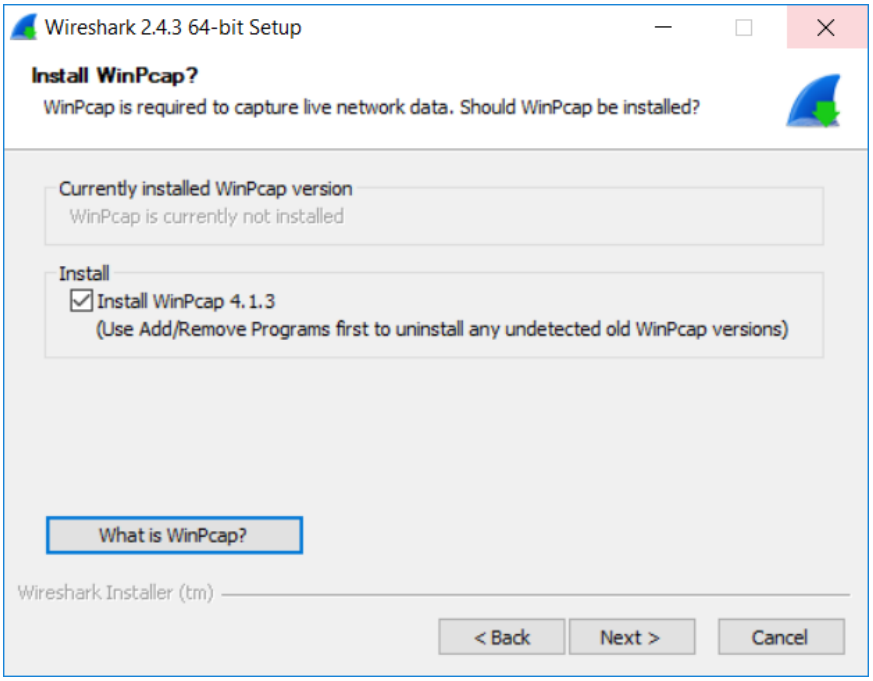

**Slika 5**

6. U ovom koraku moguće je odabrati direktorij za instalaciju alata. Nakon odabira potrebno je kliknuti ***Next***.



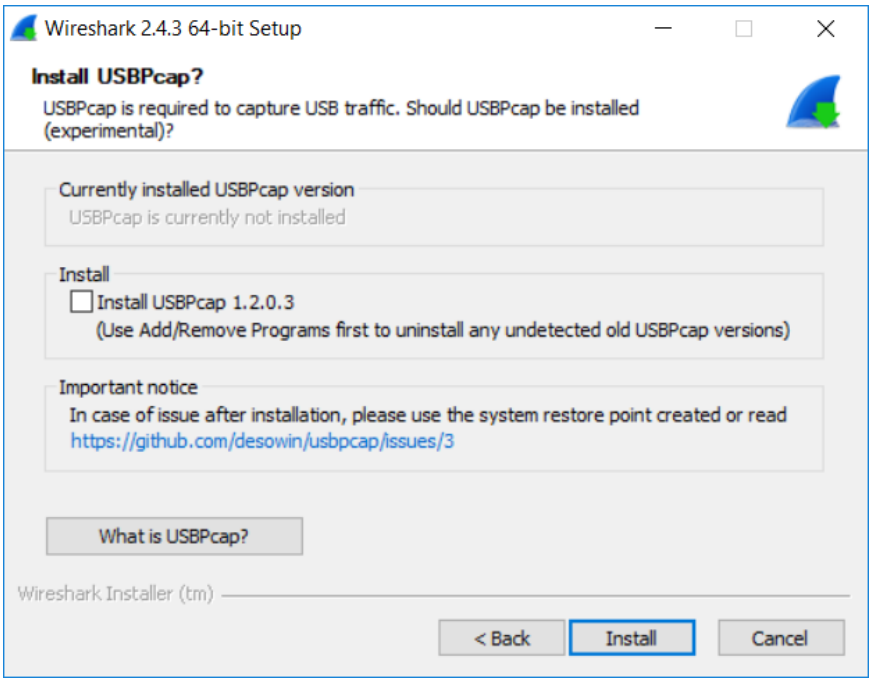

**Slika 6**

7. Kako bi Wireshark mogao snimati mrežne podatke na operacijskom sustavu Windows, potrebno je instalirati program WinPcap. Klikom na ***Next*** prelazi se na sljedeći korak.



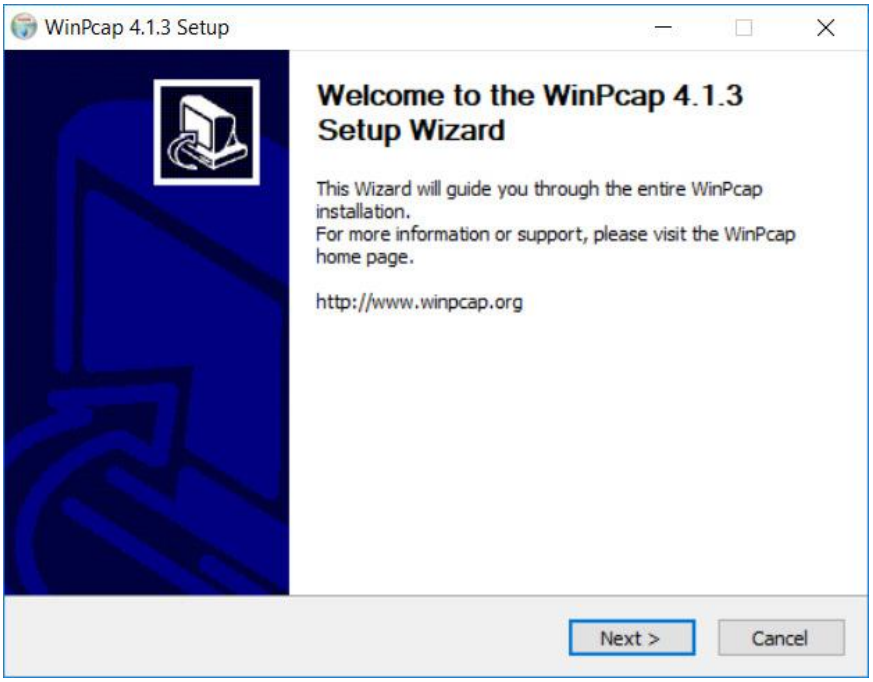

**Slika 7**

8. U ovom koraku može se odabrati i instalacija alata USBPcap za snimanje USB prometa. U ovim primjerima on neće biti potreban, pa nije označen. Klikom na ***Install*** pokreće se instalacijski prozor potrebnog programa WinPcap.



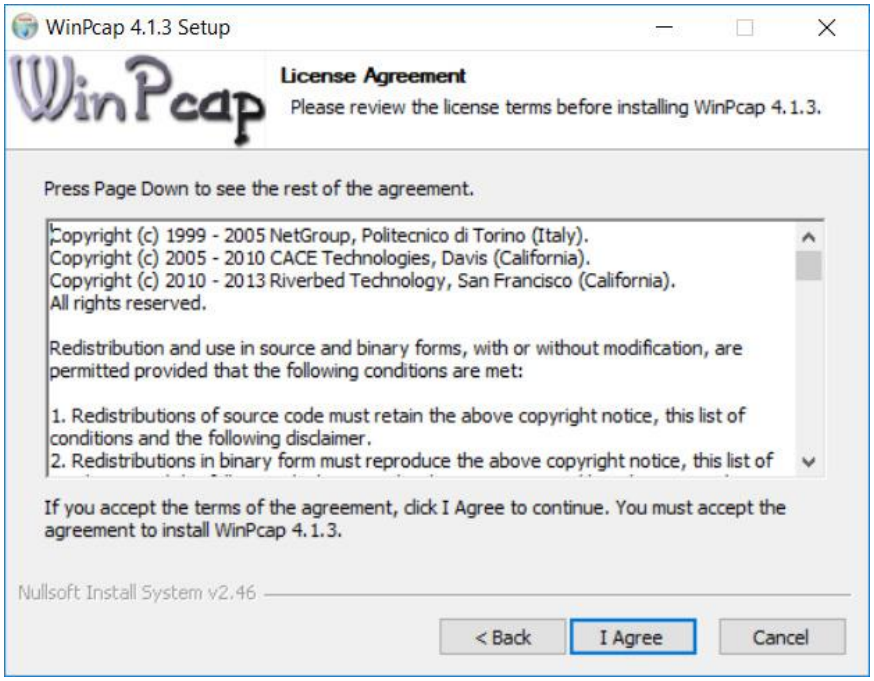

**Slika 8**

9. Zatim je potrebno stisnuti ***Next*** kako bi se prešlo na sljedeći korak.



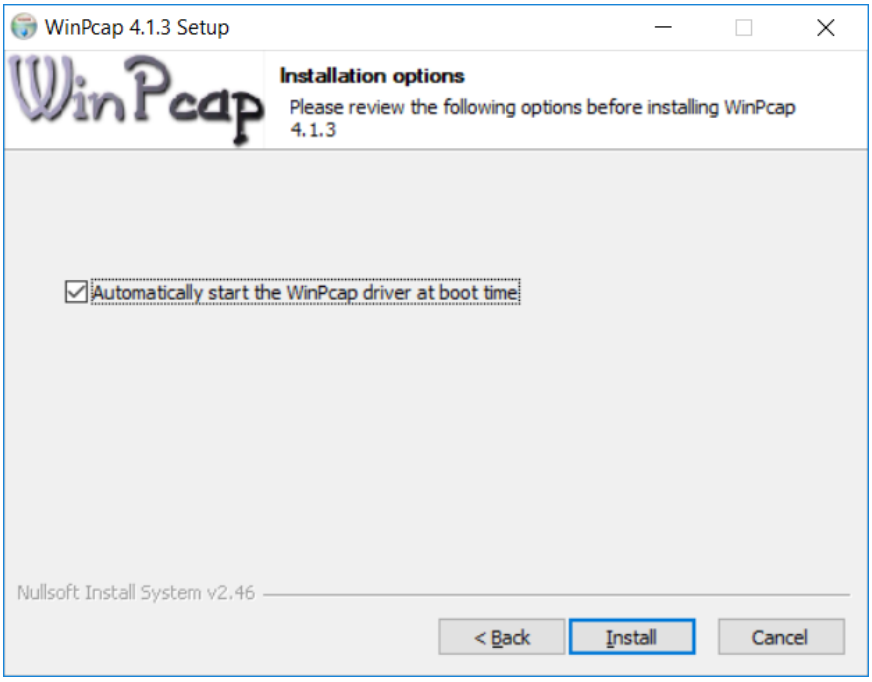

**Slika 9**

10. U sljedećem koraku potrebno je složiti se s uvjetima korištenja klikom na ***I agree***.



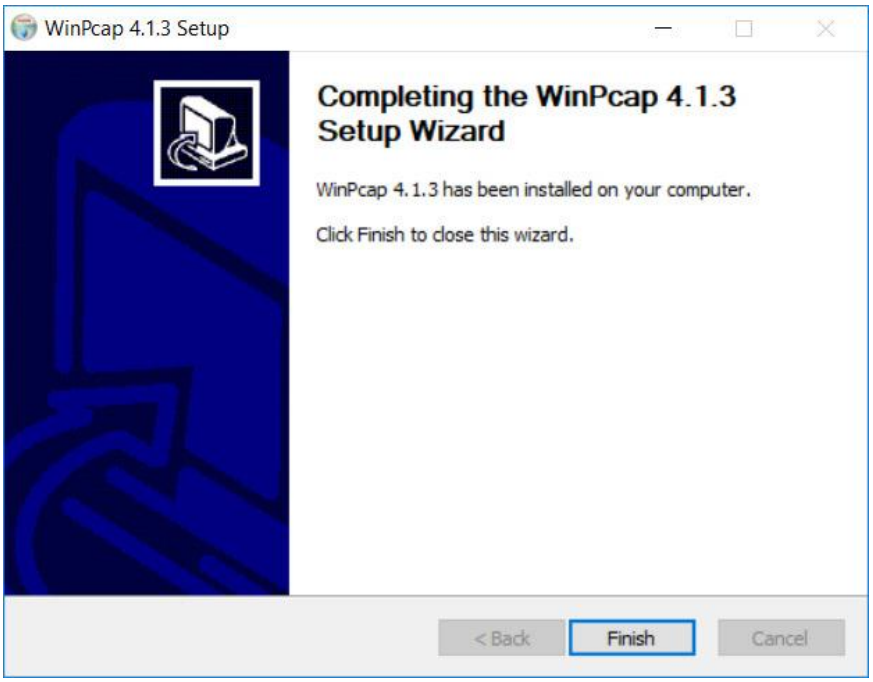

**Slika 10**

11. Klikom na ***Install*** počinje instalacija programa WinPcap.



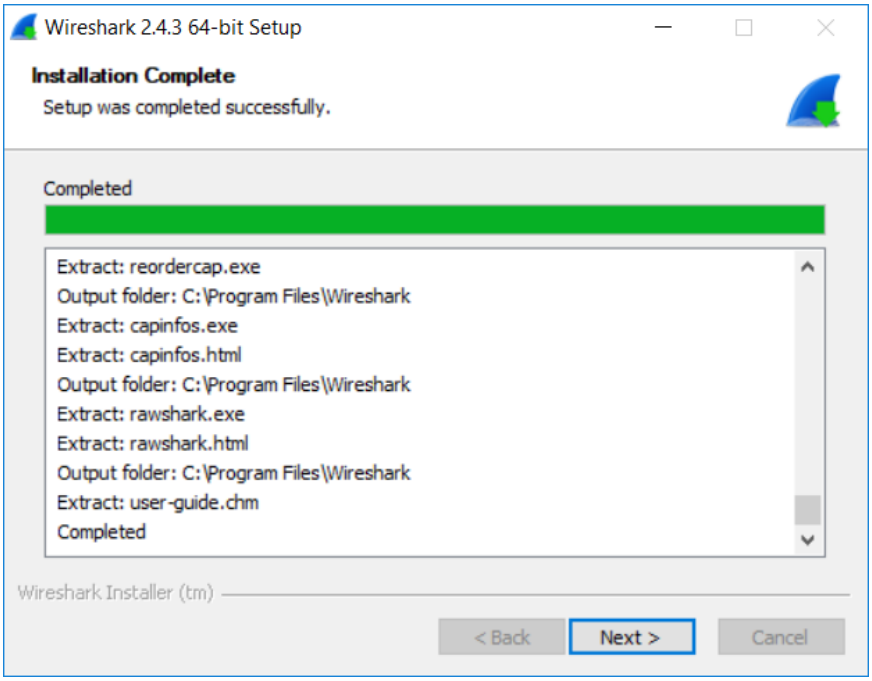

**Slika 11**

12. Nakon završetka instalacije potrebno je kliknuti na ***Finish*** kako bi se zatvorio prozor instalacije WinPcap-a i nastavila instalacija Wireshark-a.




**Slika 12**

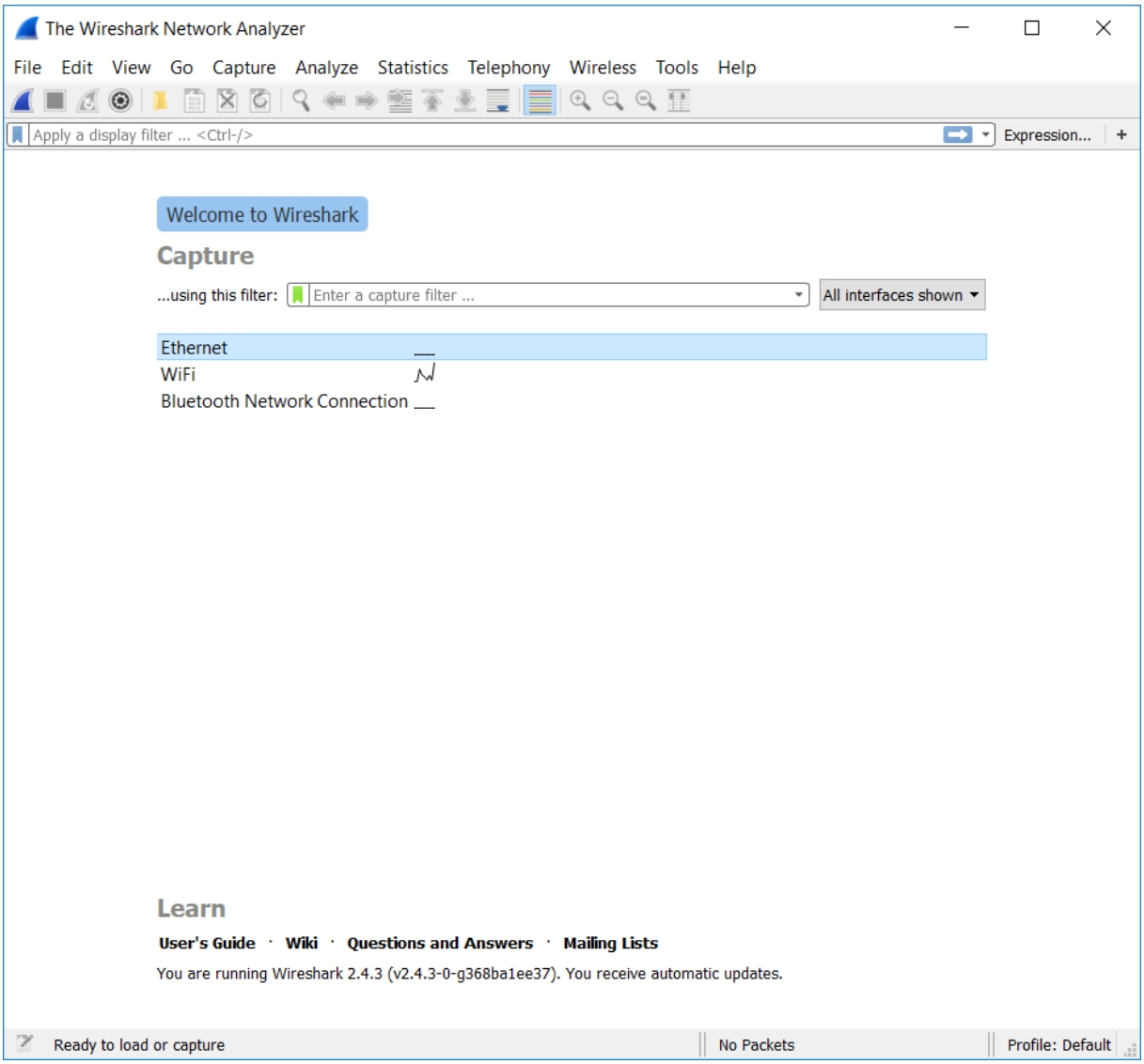
13. Nakon što je gotova instalacija Wireshark-a potrebno je kliknuti na ***Next*** te zatim ***Finish***.




**Slika 13**

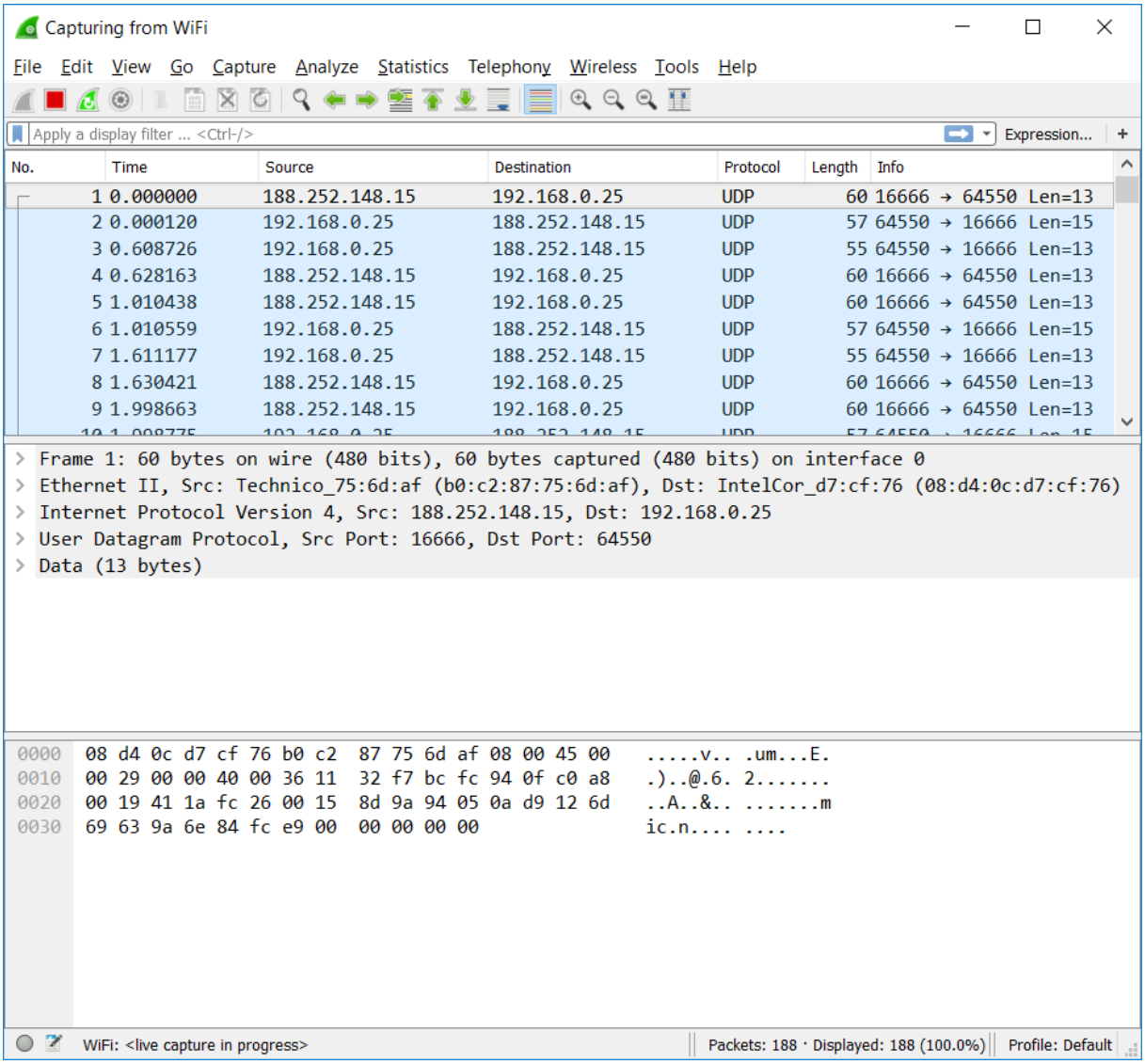
## 2.2 Korištenje

Pokretanjem Wireshark-a pojavljuje se popis mrežnih sučelja računala. U ovom primjeru računalo koristi bežičnu vezu, pa će se dvoklikom na *WiFi* pokrenuti snimanje mrežnog prometa. Početni prozor Wireshark-a prikazan je na slici 14.



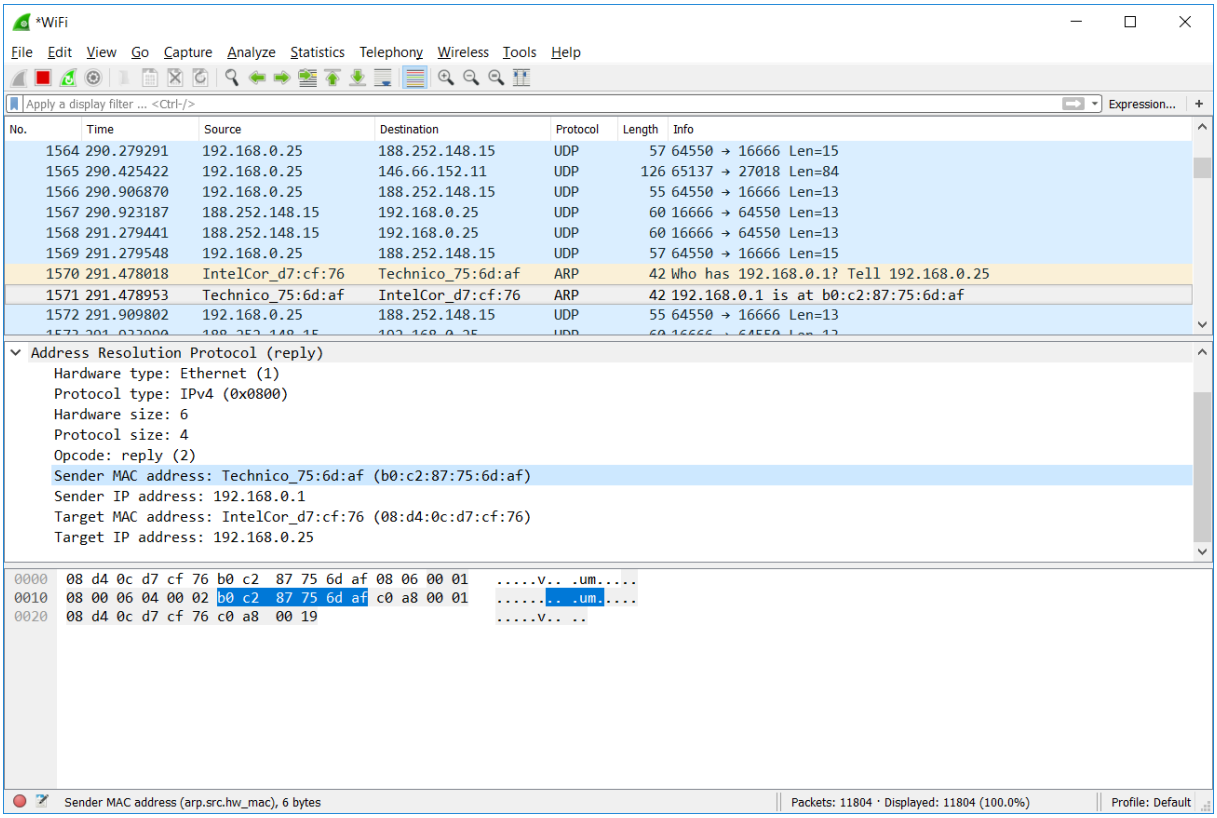

**Slika 14 – Početni prozor alata Wireshark**

Nakon toga otvara se glavni prozor alata te počinje snimanje paketa na odabranom mrežnom sučelju, kako je prikazano na slici 15. Osnovni elementi sučelja su (od vrha prema dnu) glavni izbornik, alatna traka s često korištenim radnjama, alatna traka za filtriranje, popis paketa, detalji odabranog paketa te prikaz bajtova odabranog paketa. U popis paketa dodaju se paketi kako dolaze odnosno odlaze s mrežnog sučelja.




**Slika 15 – Glavni prozor alata Wireshark**

Klikom na željeni paket, pod pretpostavkom da ga Wireshark razumije, njegov sadržaj prikazuje se u strukturiranom obliku. Na slici 16 prikazan je ARP (engl. *Address Resolution Protocol*) paket te je moguće vidjeti dijelove paketa uz nazive polja.



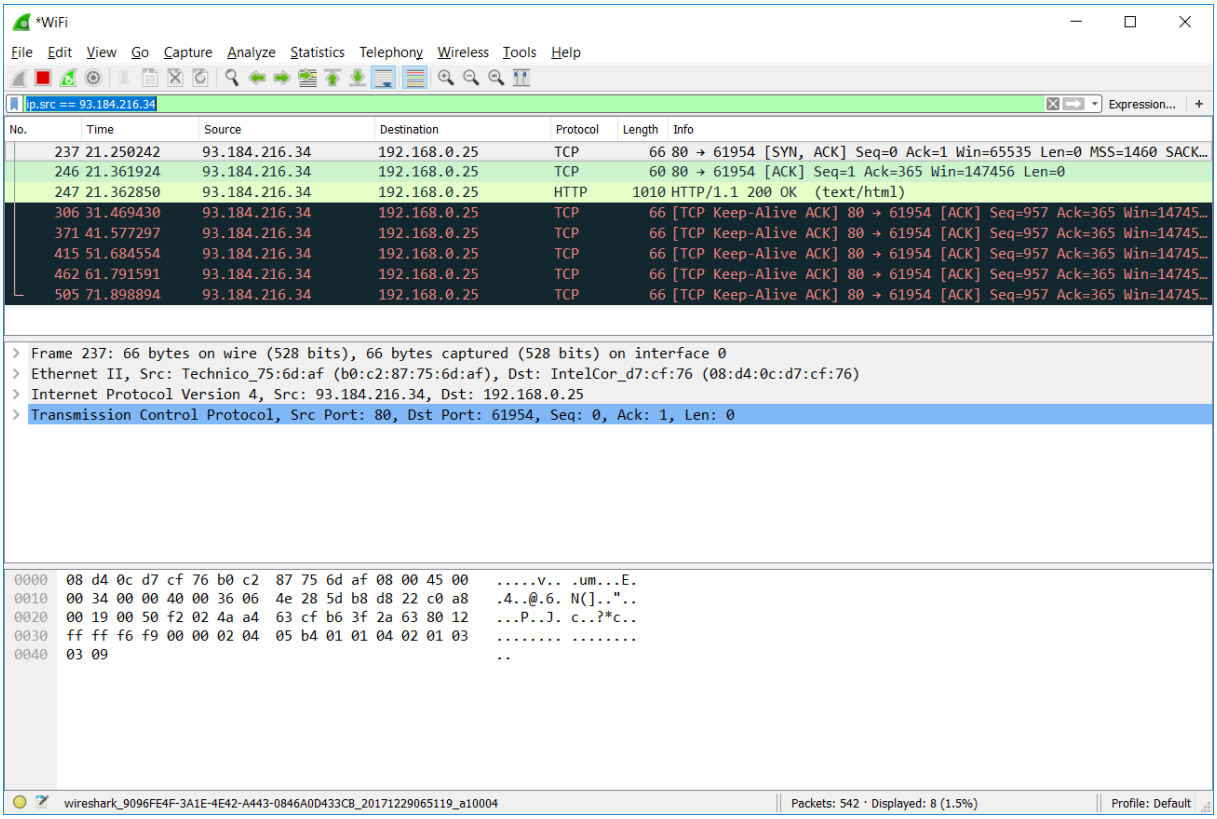

**Slika 16 – Detaljan pregled paketa**

Wireshark nudi spremanje i učitavanje snimljenih mrežnih paketa kako bi se mogli kasnije obrađivati. Kako bi se paketi spremili potrebno je zaustaviti njihovo snimanje pritiskom na crveni kvadrat u alatnoj traci te odabrati *File* → *Save* i spremiti datoteku pod željenim imenom.

### 2.2.1 Filtriranje paketa

Kako broj paketa na mreži može biti jako velik, potreban je način za lakši pronalazak zanimljivih paketa. Jedna od glavnih značajki Wireshark-a koja služi upravo za to su filteri za prikaz odnosno snimanje paketa. Pakete je moguće filtrirati po IP adresama, protokolima, priključcima (eng. *ports*), sadržaju paketa i sl.

Jednostavan i često korišten primjer je filtriranje po IP adresama. Upisivanjem „ip.src == 93.184.216.34“ u okvir za unos filtra u popisu paketa prikazuju se samo paketi kojima je izvorišna IP adresa 93.184.216.34. Ovakvo filtriranje paketa po izvorišnoj IP adresi prikazano je na slici 17.

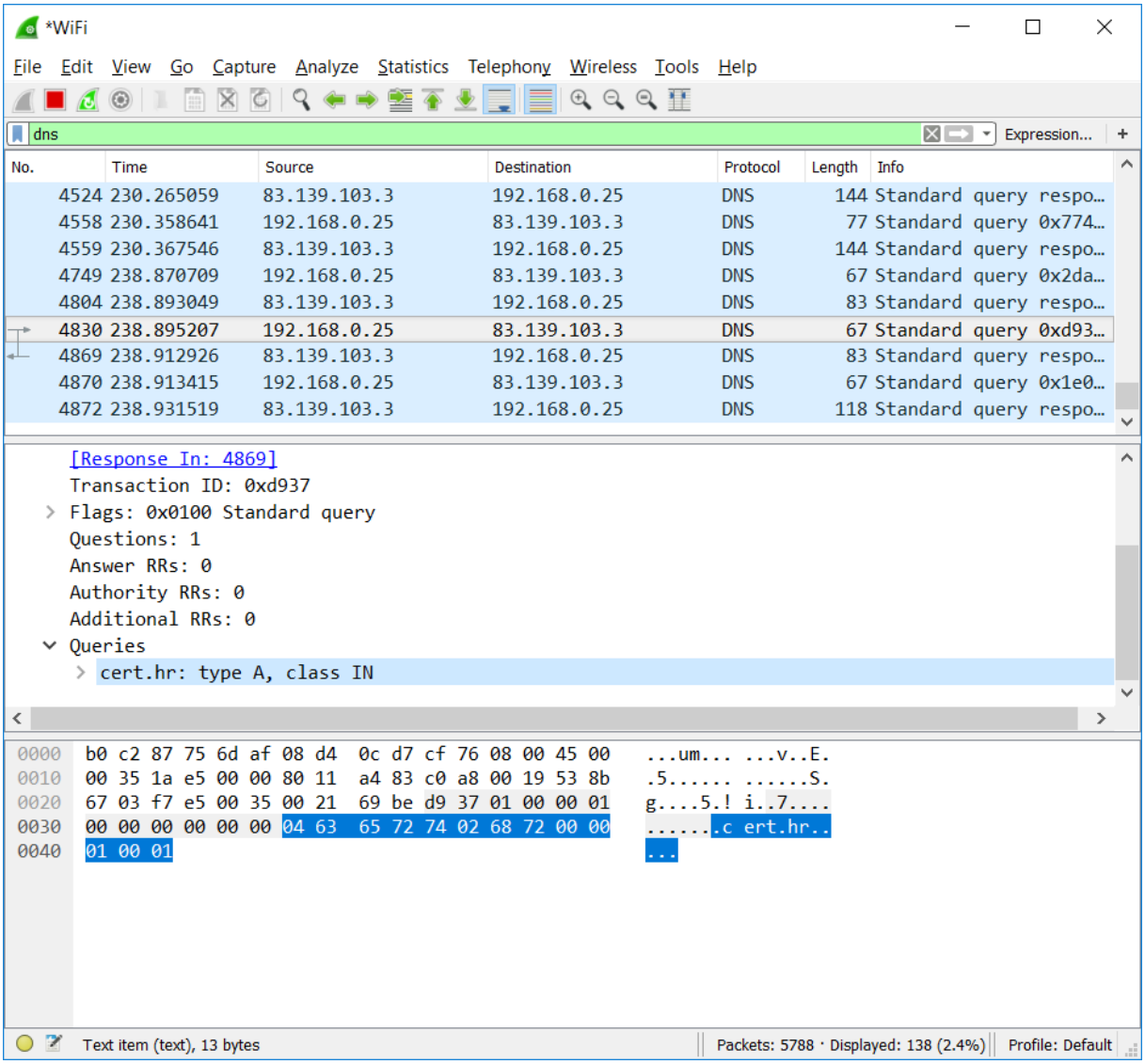



**Slika 17 – Filtriranje paketa po izvorišnoj IP adresi**

### 2.2.2 Analiza DNS prometa

DNS (eng. *Domain Name System*) je sustav koji povezuje IP adrese sa simboličkim imenima koje je lakše pamtiti. Računala međusobno komuniciraju korištenjem IP adresa, tako da računalo mora simbolička imena (npr. *cert.hr*) prije korištenja prevesti u IP adresu. Taj proces prevođenja se odvija preko mreže te ga je moguće analizirati u Wireshark-u.

Upisivanjem teksta „dns“ u polje za filtriranje u Wireshark-u prikazat će se samo DNS promet. Na slici 18 odabran je DNS upit, te je vidljivo polje upita tipa A kojim se traži IP adresa za simboličko ime *cert.hr*.

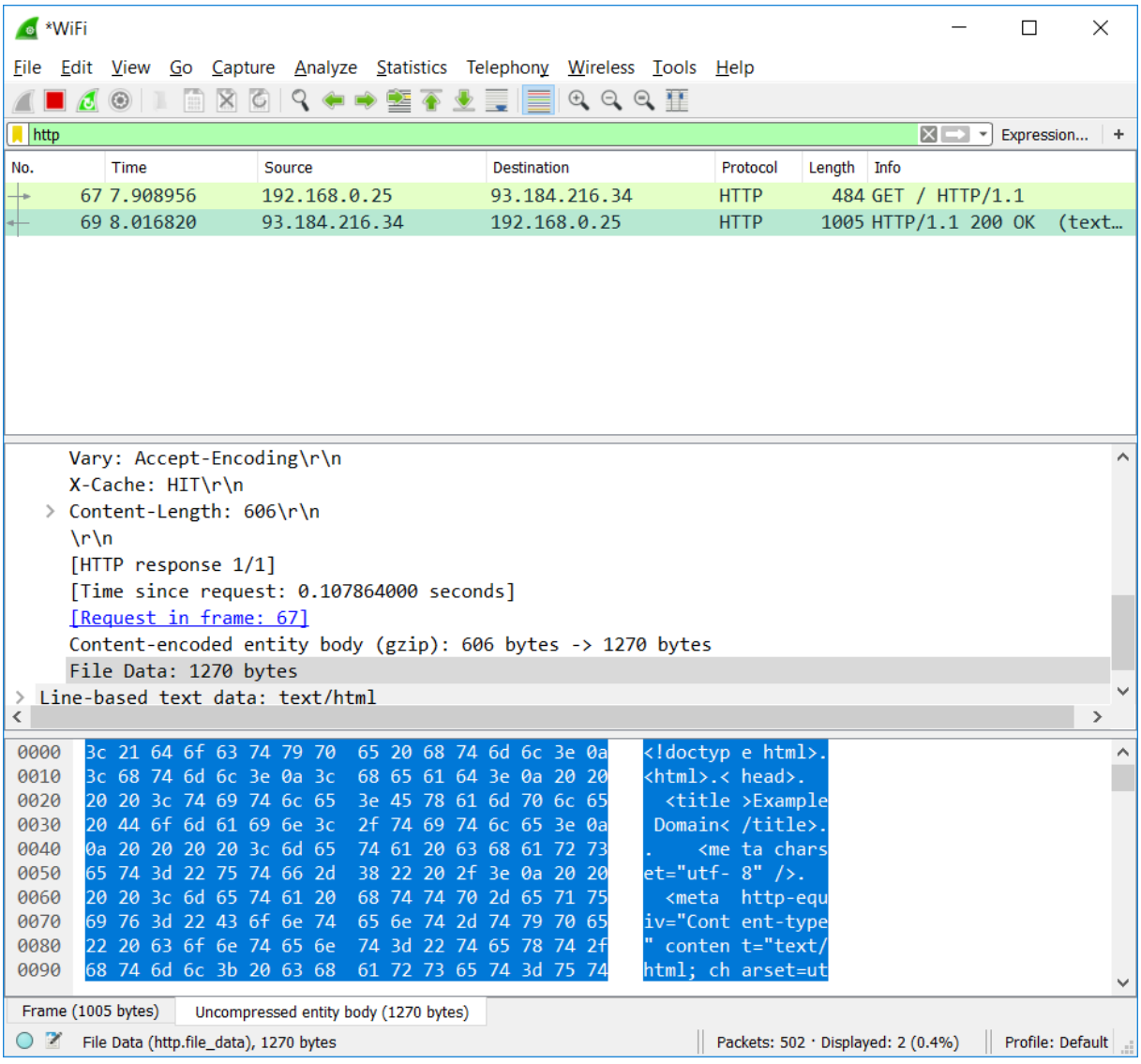



**Slika 18 – Upit DNS prevoditelju**

### 2.2.3 Analiza HTTP prometa

Protokol pomoću kojeg se prenose informacije na Webu naziva se HTTP (eng. *HyperText Transfer Protocol*). U HTTP protokolu podaci se razmjenjuju nešifrirani, tako da se korisnicima, kada god je to moguće, preporuča korištenje HTTPS protokola koji šifrira razmijenjene podatke. No, upravo zbog toga što podaci nisu šifrirani, u Wireshark-u je lako analizirati HTTP promet.

Upisivanjem teksta „http“ u polje za filtriranje prikazat će se samo paketi koje je Wireshark prepoznao kao HTTP promet. Nakon posjeta Web stranice *example.org*, u Wiresharku je moguće vidjeti HTTP zahtjev i odgovor. Na slici 19 odabran je odgovor za detaljniji prikaz. Wireshark omogućuje interaktivan pregled polja karakterističnih za HTTP protokol. Tako je primjerice odabirom polja „File Data“ moguće vidjeti HTML kod Web stranice.




**Slika 19 – Odgovor Web poslužitelja**

# 3 Zaključak

Wireshark je najpoznatiji besplatni alat za snimanje i analizu mrežnog prometa. On omogućuje detaljnu analizu velikog broja protokola te se razni IT stručnjaci svakodnevno služe njime. Mrežni arhitekti ga koriste za dizajniranje mrežnih protokola, sigurnosni stručnjaci za analizu sigurnosnih incidenata na mreži, programeri za implementaciju mrežnih protokola te ima još brojne primjene.

Wireshark je svoju primjenu našao i u edukaciji. Kako je Wireshark besplatan te se njegove osnovne značajke mogu koristiti bez puno predznanja, idealan je za upoznavanje s radom računalnih mreža.

U ovom dokumentu prikazane osnovne značajke alata Wireshark, no i one su već dovoljne za jednostavnu analizu velikog dijela mrežnog prometa.