Vježba br. 9: Analiza mrežnog prometa i mrežnih protokola

U ovoj vježbi koristimo program Wireshark, alat koji se koristi za analizu mrežnih paketa.

Grafičko sučelje programa Wireshark sadrži tri dijela u kojima se prikazuju karakteristike mrežnih paketa:
- u prvom se dijelu nalazi kratki opisi svih paketa
- u drugom dijelu se nalazi detaljan opis odabranog paketa
- u trećem dijelu se nalazi izvorni kod odabranog paketa

Zadatak 1) Pokrenite program Wireshark na sljedeći način:
sudo wireshark
te odaberite izbornik Capture - interface - eth0 - Start.
Pojaviti će se poseban prozor koji pokazuje broj i vrstu uhvaćenih paketa.
Pokrenite web preglednik i usmjerite ga na adresu www.google.com.
Nakon učitavanja cijele web stranice zaustavite hvatanje paketa:
Wireshark:Capture - Stop.
Učinite aktivnim grafičko sučelje programa Wireshark te analizirajte i zapišite sljedeće:
- Koliki je broj uhvaćenih paketa?
- Kojim sve protokolima pripadaju uhvaćeni paketi?
- Kolika je veličina u bajtovima najvećeg i najmanjeg paketa?
- Odaberite jedan paket sa SYN i ACK zastavicom, proučite ga i zapišite sve njegove karakteristike.
- Koji su izvorišni i odredišni TCP portovi korišteni kod http protokola?

Kada završite sa zadatkom obrišite sadržaj prozora odabirom izbornika File - Close.

Zadatak 2) Prekinite sve vaše mrežne aktivnosti te pokrenite hvatanje paketa:
izbornik Capture - interface - eth0 - Start.
Pustite Wireshark analizator da hvata mrežni promet nekoliko minuta.
Zaustavite hvatanje paketa:
Wireshark:Capture - Stop.
Ponovno učinite aktivnim grafičko sučelje programa Wireshark te analizirajte i zapišite sljedeće:
- Kojim protokolima pripadaju paketi koje ste uhvatili?
- Koji protokol je najzastupljeniji?
- Koji uređaji generiraju (primaju) najviše prometa?
- Koliko su zastupljeni *broadcast* paketi?

Obrišite sadržaj prozora odabirom izbornika File - Close.
Zatvorite program Wireshark.

Zadatak 3) Objasnite kako se može pomoću Wireshark analizatora prometa hvatati pakete čije odredište nisu mrežna sučelja na vašem računalu ili ne pripadaju broadcast/multicast prometu na vašoj lokalnoj mreži.