

## LABORATORIJSKA VJEŽBA BR. 7

### Analiza životnog ciklusa mrežne poruke

#### Cilj vježbe

Snimanje i analiza mrežnog saobraćaja sa ciljem provjere šta se dešava od paljenja računara do pristupa nekoj web lokaciji. Provjera koliko se teorija uklapa sa stvarnim saobraćajem.

#### Zadatak 1

##### Priprema i snimanje saobraćaja

1. Obrisati zapamćene ARP zapise:  
`arp -d`
2. Obrisati zapamćene DNS zapise:  
`ipconfig /flushdns`
3. Pokrenuti snimanje saobraćaja.
4. Pokrenuti obnavljanje IP parametara:  
`ipconfig /renew`
5. Pristupiti web adresama *www.google.com* i *www.etf.unsa.ba*
6. Zaustaviti snimanje saobraćaja

##### Analiza saobraćaja

U snimljenom saobraćaju pronaći:

(NAPOMENA: Sva odstupanja od teorije sa predavanja evidentirati)

1. DHCP pakete kojim računar traži i dobiva IP podešenja
  - a. Zabilježiti koje je podatke dobio
2. ARP saobraćaj kojim računar traži i dobiva MAC adresu default gateway
  - a. Zabilježiti MAC adresu koju je dobio
3. DNS saobraćaj kojim računar traži i dobiva IP adrese za *www.google.com* i *www.etf.unsa.ba*
  - a. Navesti IP adrese koje je dobio za *www.google.com*
  - b. Navesti IP adrese koje je dobio za *www.etf.unsa.ba*
4. TCP saobraćaj kojim se uspostavlja konekcija sa web serverima *www.google.com* i *www.etf.unsa.ba*
  - a. Zabilježiti koja od IP adresa je korištena za pristup Google
5. HTTP GET paket za Google i *www.etf.unsa.ba* (uvidom u sadržaj paketa)
  - a. Ako se ne može pronaći paket ka Google čiji je sadržaj GET zahtjev objasniti zašto
6. HTTP pakete koji predstavljaju odgovore Google i *www.etf.unsa.ba*
  - a. Koliko je ovih paketa za Google?
  - b. Koliko je obih paketa za *www.etf.unsa.ba*?
7. Analizirati HTTP konverzaciju sa *www.etf.unsa.ba* (TCP Follow stream)
  - a. Zabilježiti polja u zaglavlju HTTP upita.
    - i. Od kog host se traži objekat
    - ii. Koji objekat se traži?
    - iii. Da li se traži perzistentna konekcija?
    - iv. Kako se predstavlja web preglednik?
    - v. Koji jezik preferira?

- b. Zabilježiti polja u zaglavlju HTTP odgovora
  - i. Kako se Web server predstavlja?
  - ii. Koristi li cookie?
  - iii. Kako je odgovor kodiran?
- 8. U nekom paketu provjeriti udaljenost u bajtima od početka paketa do IP adrese odredišta i izvorišta
  - a. Provjera pitanja i odgovora sa ispita.

Ovakvo snimanje i analiza saobraćaja na vašim računarima kod kuće je četvrta zadaća koju treba predati u elektronskoj formi kao (.pdf) prilog putem Zamgera do nedjelje 03.05.2015. do ponoći.

Priprema:

M.Eng. Amer Zec

M.Eng. Alvin Huseinović

Sarajevo, 21.04.2015. godine