Poročilo za vajo *Zajemanje in analiza TCP/IP prometa z orodjem Wireshark*

1. ARHITEKTURA MERILNEGA OMREŽJA

Identificirajte vrste fizičnih povezav med posameznimi elementi in odgovorite na naslednja vprašanja.

1.1.V tabelo vpišite vrsto kabla uporabljenega za dano povezavo:

Povezava	Vrsta kabla
računalnik-stikalo	
računalnik-računalnik	

1.2. Ugotovite naslov IP svojega terminala (računalnika)?

_____.

1.3. Zakaj je v topologiji uporabljeno stikalo (angl. switch)?

_____.

1.4. Če bi stikalo zamenjali s koncentratorjem (angl. hub), kako bi ta sprememba vplivala na rezultate zajema prometa z uporabo orodja Wireshark?

_____.

2. ZAJEM SPLOŠNEGA PROMETA – NAVADNI NAČIN

2.1. Izpolnite naslednjo tabelo in odgovorite na spodnja vprašanja.

Vrsta prometa	**Vrste protokolov v zajeti sledi (naštejte in hierarhično uredite)**	**Povprečna velikost PDU**	**Povprečna pasovna širina [b/s]**	**Število in odstotek TCP PDU**	**Število in odstotek UDP PDU**
Splošni					

2.2. Poglejte ponorni naslov prejetih paketov. Kakšna sta ponorni (destination) IP in ponorni (destination) MAC naslov?

ponorni MAC naslov:_____;

ponorni IP naslov:_____.

2.3. Katere protokole transportnega sloja opazite in kakšno je statistično razmerje med njimi?

_____.

3. ZAJEM IN FILTRIRANJE HTTP PROMETA

3.1. Izpolnite naslednjo tabelo in odgovorite na spodnja vprašanja.

Vrsta prometa	Vrste protokolov v zajeti sledi (naštejte in hierarhično uredite)	Povprečna velikost PDU	Povprečna pasovna širina [b/s]	Število in odstotek TCP PDU	Število in odstotek UDP PDU
Spletni					

3.2. Katere (nove) protokole opazite, v primerjavi s prejšnjo nalogo?

_____.

3.3. Opišite protokolno strukturo (protokole, ki so specifični) za prenos spletnih vsebin?

_____

_____.

3.4. Ali je iz vsebine izločenega prometa razvidna vsebina obiskane strani?

_____.

3.5. Poiščite vtipkano vsebino (iskalne parametre za npr. Google, ali Wikipedio). Uporabite funkcijo iskanja znakovnega niza. Ali so vpisani podatki razvidni iz zajetega prometa?

_____

_____.

3.6. Prepišite vrstico z najdenim nizom (zaporedna številka, izvorni in ponorni MAC naslov, izvorni in ponorni IP naslov) :

_____

_____.

Dodatek: Na enak način lahko poiščete geslo za vstop do strani, ki ne kriptirajo prenosa podatkov (npr: http://www.mail386.com/).

_____

_____.

4. ZAJEM IN FILTRIRANJE VIDEO PROMETA

4.1. Izpolnite naslednjo tabelo in odgovorite na spodnja vprašanja.

Vrsta prometa	Vrste protokolov v zajeti sledi (naštejte in hierarhično uredite)	Povprečna velikost PDU	Povprečna pasovna širina [b/s]	Število in odstotek TCP PDU	Število in odstotek UDP PDU
Spletni					

4.2. Kakšna je deklarirana pasovna širina video vsebine (poiščite jo v izbirniku MS Media Playerja: *File* → *Properties*). Ali se deklarirana in povprečna uporabljena pasovna širina ujemata?

_____.

4.3. Katere protokole transportnega sloja opazite in kakšno je statistično razmerje med njimi?

_____.

4.4. Kakšne razlike opazite v protokolni strukturi (vrste uporabljenih protokolov) pri prenosu spletnih vsebin in video vsebin?

_____.