# 5.vaja: Zajem mrežnega prometa.

Vohljač (sniffer) je program ali naprava, ki omogoča opazovanje/zajem prometa prek omrežja. Med najbolj priljubljeno programsko opremo na tem področju sodi Ethereal, ki se je leta 2006 zaradi zaščite blagovne znamke preimenoval v Wireshark.

Kaj je to vohljač, kje se uporablja, kakšne vrste vohljačev poznamo si preberite v članku na spletni strani:

<http://www.mojmikro.si/v_praksi/mojster/umetnost_vohljanja_po_prometu>

Izdelava vaje:

1. Z interneta prenesite program Wireshark in ga namestite na računalnik.
2. Zajemite promet, ki prihaja iz vaše mrežne kartice in ga shranite za kasnejšo analizo.
3. Na računalniku poženite ukaz ping na naslov 193.189.160.13, v programu Wireshark nastavite filter tako, da spremljamo le icmp pakete in zajemite promet.
4. Priklopite vaš in sosedov računalnik na ethernet hub. Sosed naj zažene ping 193.189.160.13, vi pa s pomočjo filtra glede na njegov ip naslov nastavite zajemanje le njegovih paketov.
5. Analizirajte promet, ki ste ga zajeli pri točki 2 (MAC naslov, IP naslov, vrsta protokola).

Vprašanja:

1. Na kratko opišite delovanje vohljača (sniffer-ja).
2. V kakšne namene se uporabljajo t.i. vohljači?
3. Naštejte vsaj tri dobre lastnosti uporabe programa Wireshark.
4. Naštejte vsaj tri vrste filtrov, s katerimi lahko filtriramo zajet promet?
5. Kaj je potrebno storiti na omrežnem stikalu, da lahko prestrežemo sosedov promet?

Priprava doma:

1. Preberite članek v reviji Moj mikro.
2. Pojdite na wiresharkovo stran (http://www.wireshark.org/). Poglejte si video Introduction To Wireshark.
3. Potegnite program Wireshark z interneta in ga instalirajte na svoj računalnik. Pojdite čez osnovne menije, ugotovite, kako zajemate podatke, nastavite filter, …