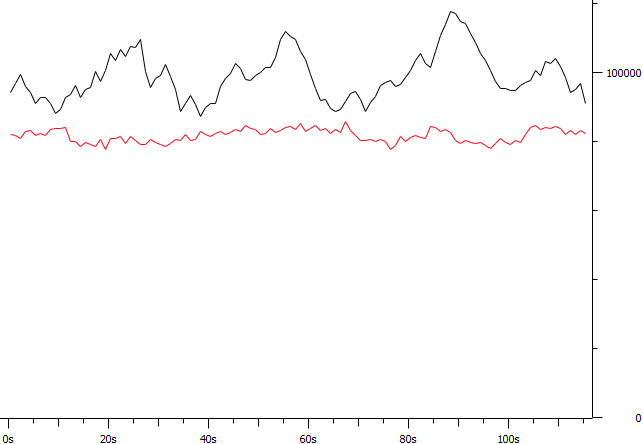
**Ako porovnať 2 pcapy vo Wiresharku**

**Prečo to chceme spraviť?**

Ak si chceme porovnať 2 pcapy, aby sme videli rozdiely napríklad v intenzite tokov. S príkladom použitia sa môžete stretnúť na cvičení, v ktorom sa preberajú mechanizmy pre tvarovanie a orezávanie sieťovej prevádzky. Napríklad na tomto obrázku vidíme orezanie prevádzky nad hodnotu 84 000 bit/s.



Obidva čiarové grafy pochádzajú zo svojho vlastného pcapu, t.j. neboli spustené 2 toky naraz, ale najskôr bol pustený jeden a potom druhý. Pri prvom (**čiernom**) nie je nastavená žiadna politika, je to reálny tok, ktorý sieťou v danom momente prechádza. Druhý (**červený**) graf je ukážkou ako funguje politika. Odporúčame nastaviť si pre každý takýto tok iné číslo portu, pretože inak by Wireshark nerozpoznal, že ktorý tok je ktorý. Možno by to vedel odlíšiť použitím nejakého vhodného filtra, no tento spôsob je určite jednoduchší.

Ešte odporúčame pri takomto porovnávaní odfiltrovať si len pakety nášho toku a uložiť len tie.

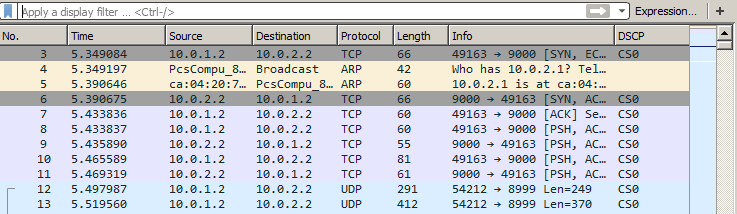
Odchytíme si nejakú sieťovú prevádzku. V našom prípade bude prvý tok mať port **8999** a druhý tok bude mať port **9001.** Takže si nastavíme želané filtre: **udp.dstport == 8999** pre prvý tok a potom pre druhý tok bude filter **udp.dstport == 9001.**

Nesmieme zabudnúť stopnúť odchytávanie paketov červeným štvorčekom, lebo inak nemáme možnosť si daný **pcap** súbor uložiť.

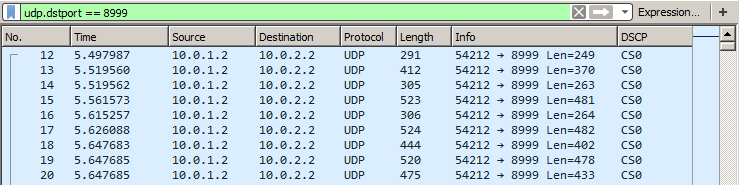
Ukážka len pre tok s portom 8999. Pri toku s portom 9001 postupujeme úplne rovnako.

V oboch prípadoch zobrazujeme od prvého paketu. Vidíme, že tok UDP začína niekde od piatej sekundy.

Pôvodná prevádzka bez filtra:



Odfiltrovaná prevádzka:

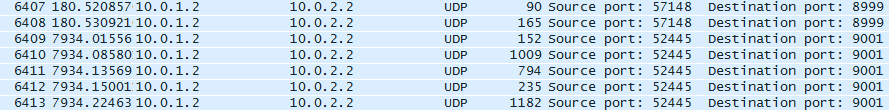


Uložíme len tieto pakety, vo Wiresharku klikneme na **Export Specified Packets** v karte **File.**

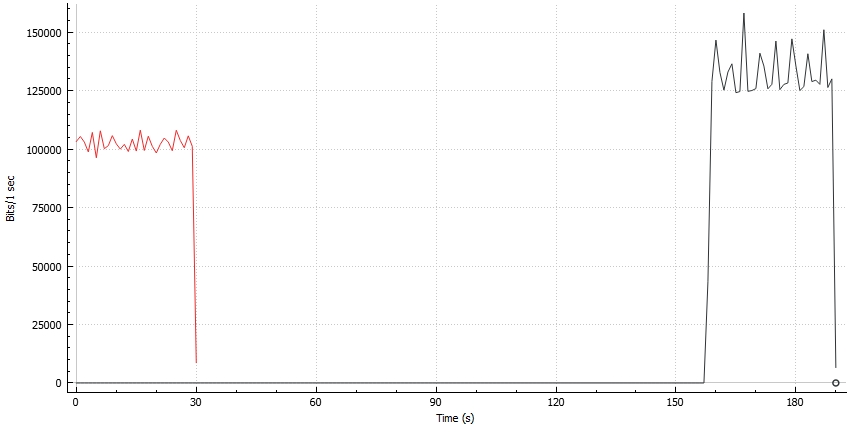
**Porovnávanie:**

**1.** otvoríme si jeden pcap súbor, je úplne jedno ktorý.

**2.** klikneme na tlačidlo **Merge...** v karte **File** a otvoríme si druhý pcap. Obidva pcapy sa nám spoja dohromady. Bohužiaľ Wireshark to spraví tak, že najskôr dá 1 tok, potom druhý, ale medzi nimi dá obrovskú časovú medzeru. Na tomto obrázku môžeme vidieť prvý paket druhého toku a čas (cca 7934 s.), v ktorom sa vyskytuje:



Takto ale nedostaneme želaný výsledok, pretože výsledný graf vyzerá nasledovne:





Preto musíme na prvom pakete (nájdeme si ho ručne) zaškrtnúť po kliknutí pravým tlačidlom **Set/Unset Time Reference** alebo len stlačíme kombináciu **Ctrl+T**. Všimneme si, že čas druhého toku ide ako keby od 0 a to sme presne chceli. Výsledný graf potom vyzerá takto:

