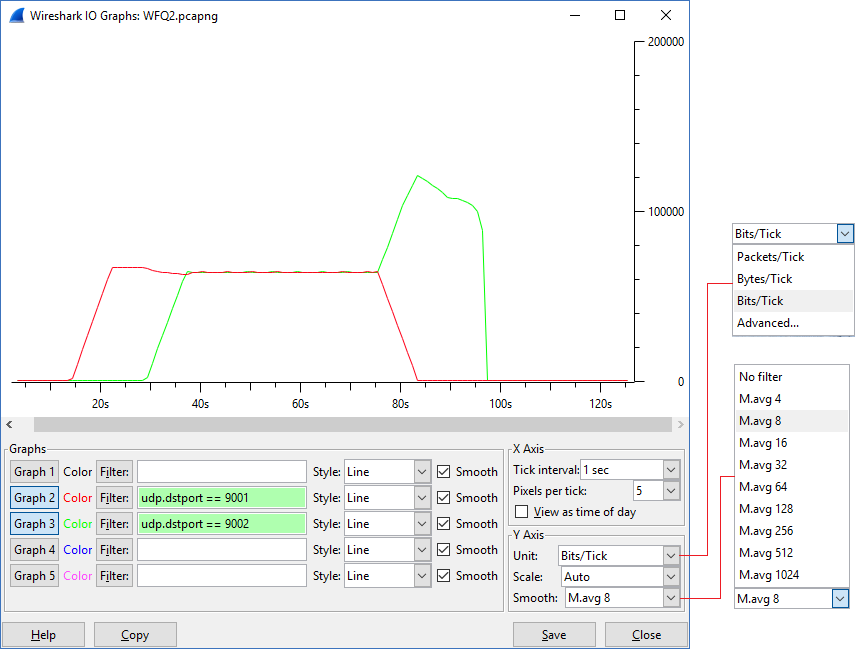
## Ako efektívne využívať program Wireshark v predmete OKS

### Staršia verzia program WS 1.12.7

Program Wiresharkmôžeme považovať za nevyhnutnú súčasť každého z cvičení. Pomocou neho a jeho funkcie IO Graph si vieme zobraziť naše vygenerované dáta a tým ich aj dôkladne preskúmať. Máme k dispozícií rôzne filtre, ktoré môžeme použiť. Vieme si nastaviť čiarový graf pre každý jeden tok, ktorý chceme sledovať. Máme k dispozícií filtre vyhladzovania prevádzky, napríklad M.avg 4, M.avg 8, M.avg 16 atď. Znamená to, že I/O Graph nezobrazí jeden pixel za okamih (1 pixel per tick), u nás je týmto jedným okamihom jedna sekunda, ale zobrazí ich 4, 8, 16 atď., za jeden okamih, spraví z nich priemer a toto potom zobrazí. Niekedy to veľmi pomôže, pretože ak nemáme konštantný tok, sú tam veľké výkyvy a nevieme z toho presne určiť to, čo v grafe chceme nájsť. *Obrázok 4.6* zobrazuje okno I/O grafu, kde môžeme vidieť nastavenia filtrov zobrazovaných tokov (UDP 9001 a 9002) a tiež nastavenia vyhladzovania (M.avg 8). Na osi X je čas, na osi Y sa nacházajú bity za sekundu.

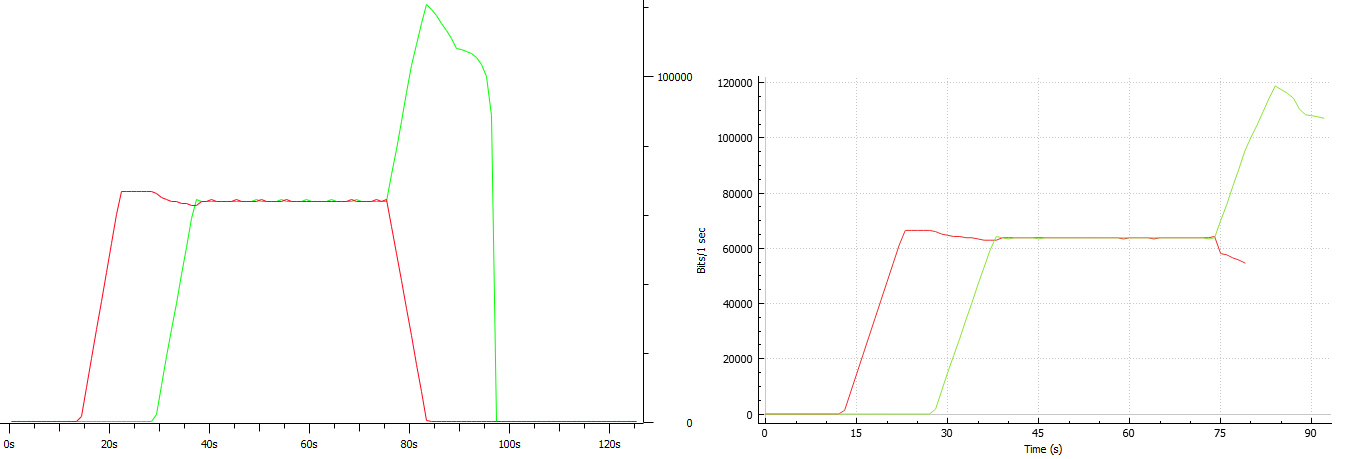


*Obrázok 4.6 Nastavenie filtrov a vyhladzovania vo Wiresharku 1.12.7*

### Aktuálna stabilná verzia (2.2.4) a jej výhody

Dostala sa nám do rúk nová verzia Wireshark 2.2.4, ktorej funkcia I/O Graph má niektoré vylepšenia a trocha nám uľahčí prácu. Zhrnieme jeho výhody a zvýrazníme, ktoré z nich sú podstatné pre cvičenia z predmetu OKS.

Za prvú veľkú výhodu môžeme považovať zmenu zobrazovania grafov a schopnosť programu vedieť približovať a oddiaľovať krivku, ktorú skúmame. Vieme si tým lepšie zistiť, že akú hodnotu nadobúda graf v konkrétnom čase. Ďalším vítaným vylepšením je schopnosť programu ponechať si užívateľom definované filtre, ktorými filtrujeme jednotlivé toky, takže ich nemusíme pri každom meraní znova a znova písať, tak ako to bolo v staršej verzii. Malou nevýhodou pri týchto filtroch je, že sa nedajú posúvať v zozname filtrov hore a dole. Vyhladzovanie je tiež trochu iné, ale v princípe znamená to isté. 10 interval SMA = M.avg 8, kde SMA je jednoduchý kĺzavý priemer. Pre porovnanie si ukážeme obrázky vyhladeného toku pomocou M.avg = 8 na obrázku *Obrázok 4.7*.



*Obrázok 4.7 I/O graf vo verzii 1.12.7 (vľavo) a vo verzii 2.2.4 (vpravo)*

Môžeme si všimnúť, že grafy sú veľmi podobné, ale v novšej verzii nevidíme ten moment, kedy tok zanikne. Taktiež si môžeme všimnúť, že v novšej verzii nám pribudla mriežka, vďaka ktorej vieme lepšie odhadnúť aké hodnoty máme z grafu vyčítať. Nedá sa nastaviť hustota mriežky, resp. ak sa dá, zatiaľ sme nezistili, že ako. Nechýba ani pomenovanie osí X a Y, ktoré nám v predošlej verzii chýbalo. Vidíme, že na osi X máme čas, na osi Y budeme veľmi často používať bity za sekundu.

Vidíme, že pravý graf je trošku viac natiahnutý do strany, ľavý graf je viac natiahnutý do výšky. Je to spôsobené tým, že pravý graf je flexibilnejší a lepšie sa vie prispôsobiť zmenšovaniu a zväčšovaniu okna grafu. Výhodou oproti staršej verzii je tiež možnosť navoliť si až 22 farieb grafu, kdežto pred tým sme mali k dispozícii len 5 prednastavených farieb (čiernu, červenú, modrú, zelenú a ružovú). Typ ani hrúbku čiary si nevieme sami nastaviť, ale vnímame to ako vhodné doplnenie do novej verzie.

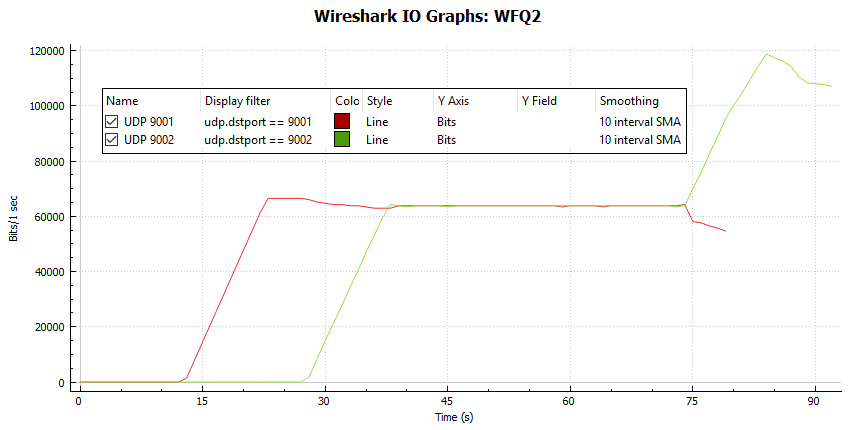
*Tabuľka 4.2 Porovnanie vybraných funkcií programu Wireshark ver. 1.12.7 a ver 2.2.4 využívaných v predmete OKS*

|  |  |  |
| --- | --- | --- |
| **Funkcia** | **Ver. 1.12.7** | **Ver. 2.2.4** |
| Možnosť priblížiť si I/O graf | nie | áno |
| Prítomnosť mriežky v grafe | nie | áno |
| Flexibilita grafu pri zmenšovaní/zväčšovaní okna | nie | áno |
| Ponechanie nastavených filtrov aj po vypnutí programu | nie | áno |
| Počet farieb | 5 | 22 |
| Pomenovanie osí | nie | áno |

### Odporúčanie ako efektívne zobrazovať I/O grafy vo WS

Každé jedno z cvičení obsahuej minimálne jeden graf. Reporty z cvičení, ktoré študenti odovzdávali v r. 2016 ako vypracovanie daného zadania ukázali, že ich výstupy sú veľmi zle ciťateľné, alebo veľmi zle popísané, alebo oboje, prípadne nemajú nastavené rovnaké parametre zobrazovania (napríklad vyhladzovanie), keď porovnávajú dva alebo viaceré grafy z rôznych scenárov navzájom. Preto vznikla potreba, spraviť odporúčanie pre zobrazovanie a ukladanie grafov, ktoré by bolo potrebné zaradiť hneď na prvé cvičenie. Ukážeme si ako najefektívnejšie tieto grafy uložíme ako obrázky tak, aby boli dobre čitateľné. Keď chceme graf exportovať ako obrázok formátu .png, výsledok by bol taký, ako ilustruje *Obrázok 4.8*. Samozrejme, nesmieme zabúdať ani na popis používaných filtrov, prípadne vyhladzovaní. Graf má automaticky nastavený názov. Tento názov korešponduje s názvom .pcap súboru, ktorý sme si uložili a graf z neho vykreslili. V porovnaní s nami odfoteným grafom je horšie čitateľný, predovšetkým jeho X a Y osi.

Na základe skúseností, odporúčame grafy robiť buď pomocou Nástroja na vystrihovanie (Snipping Tool), ktorý je súčasťou OS Windows, alebo pomocou snímky obrazovky.



*Obrázok 4.8 Ukážka grafu s použitím filtrov a vyhladzovaní*