



Számítógép hálózatok

12. gyakorlat

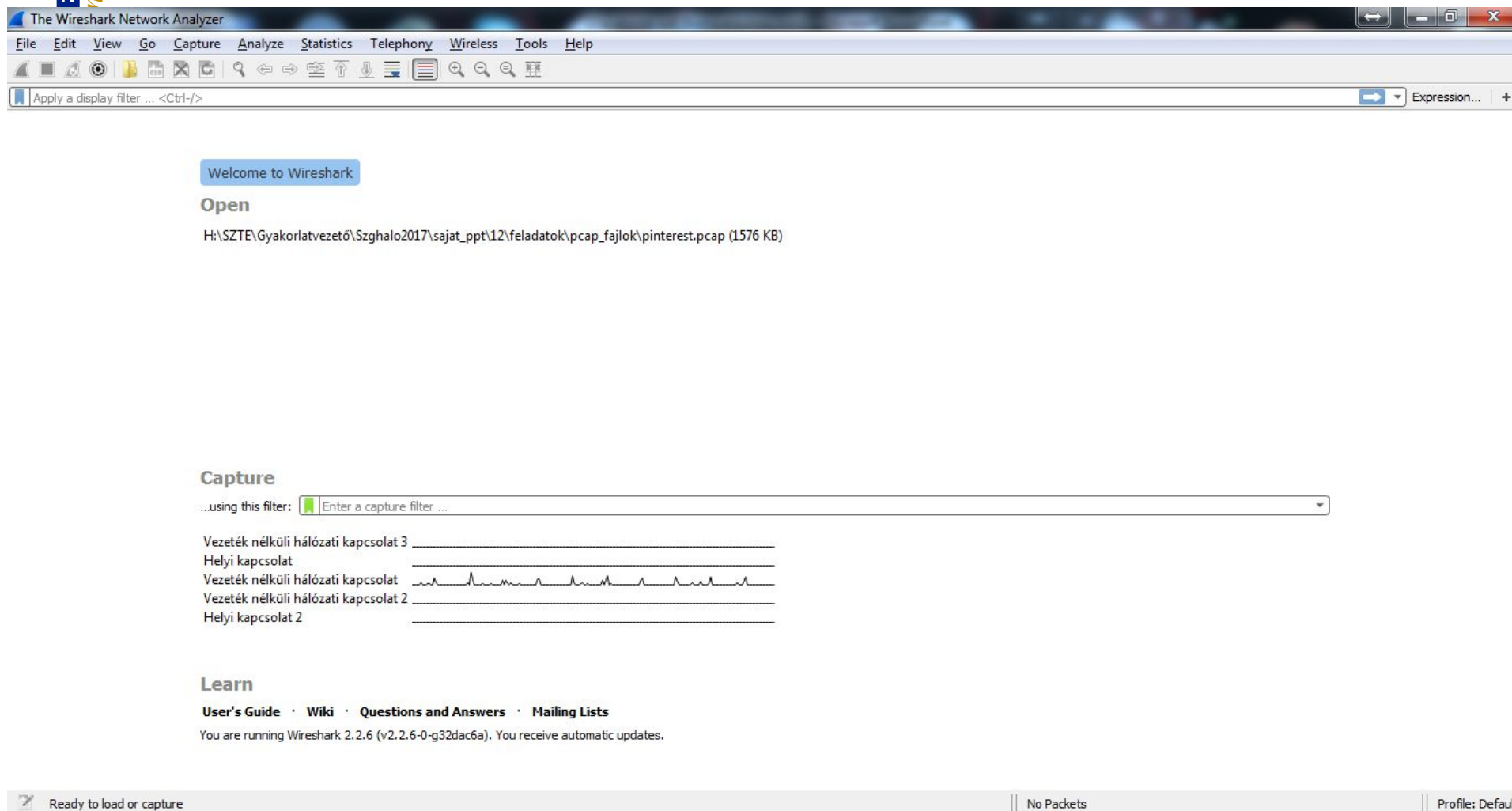


Mi a Wireshark?

- ▶ Ingyenes program!!!
- ▶ Egy hálózati forgalom megfigyelő és elemző eszköz
- ▶ Segítségével elfoghatjuk és elemezhetjük a hálózaton közlekedő csomagokat
- ▶ Többféle felhasználási mód:
 - Hálózati-, biztonsági problémák felderítése, hálózat működésének megértése

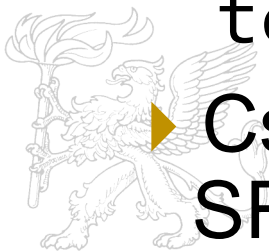


Wireshark indítása



Elfogás közbeni szűrők (Capture Filter)

- ▶ Segítségükkel szűkíthetjük a elkapni kívánt csomagok körét
- ▶ Általános alakja:
`[not] primitive [and|or [not] primitive ...]`
- ▶ Pl. csak a 22-es (SFTP/SSH) port forgalmát fogja el
`tcp port 22`
- ▶ Csak a 10.0.0.5 IP címre és címről érkező SFTP/SSH csomagokat fogja el
`tcp port 22 and host 10.0.0.5`



Elfogás közbeni szűrők (Capture Filter)

- ▶ Szűrő primitívek:
- ▶ http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html#ChCapExFilt2
- ▶ További példák szűrő kifejezésekre:
- ▶ <http://wiki.wireshark.org/CaptureFilters>



Capture filter vs. Display filter

- ▶ Szűrés mindkettő, de nem tévesztendő össze!
- ▶ Első lépésben elfogunk, második lépésben megjelenítünk
- ▶ A megjelenítéssel szabályozhatóak a fájlba írt csomagok száma



Munka az elfogott csomagokkal

- ▶ A megfigyelés elindítása után valós időben listázódnak az elfogott csomagok
- ▶ Az alapvető információkat leolvashatjuk ebből a listából (küldő, fogadó címe, protokoll típusa)
- ▶ Bővebb információt kaphatunk a megfelelő sorra kattintva
 - Duplán kattintva új ablakban nyílik



Munka az elfogott csomagokkal

- ▶ A fejlécre jobb gombbal kattintva az előugró menüvel rendezhetjük a csomagokat
- ▶ A lista csomagjaira kattintva további hasznos funkciókat érhetünk el, pl.:
 - **Apply as Filter:** a kiválasztott csomag alapján szűrőt hoz létre és azt alkalmazza a listára



Elfogott csomagok további szűrése

- ▶ A már elfogott csomagok között tovább szűrhetünk különböző szempontok szerint: adott protokollra, egy mező megléte szerint, egy mező értéke szerint...
- ▶ Ebben az esetben a szűrőfeltételnek nem megfelelő csomagok a listában maradnak, csak rejtve lesznek
- ▶ Pl: egy adott IP címre/ről jövő csomagok
ip.addr==192.168.0.1



Megjelenítési szűrők néhány példa

- ▶ A 25-ös (SMTP) port csomagjait jelenítsük csak meg

tcp.port eq 25

- ▶ Csak a 10.0.0.5 címről érkező csomagokat mutassuk meg

ip.src==10.0.0.5

- ▶ További példák:

<http://wiki.wireshark.org/DisplayFilters>

- ▶ Szűrő primitívek referenciája:

<http://www.wireshark.org/docs/dfref/>




Szűrő kifejezések létrehozása

- ▶ Ha még nem megy fejből a szűrőkifejezések írása, akkor segítségünkre lehet a „Filter expression” dialógusablak
 - Analyze → Display filters... → Expression...
- ▶ Itt protokollok szerint rendezve megtalálhatók a mezőnevek és a relációk
- ▶ Létrehozás után el is menthetjük a későbbi egyszerű használat érdekében.
- ▶ A listában találhatunk előre megírt kifejezéseket is.

Csomagok keresése

- ▶ Lehetőség van egy konkrét csomag megkeresésére.

Edit → Find packet... (vagy a  ikon az eszköztárban)

- ▶ Kereshetünk szűrő alapján, byte szekvencia szerint illetve egy adott szövegrészre



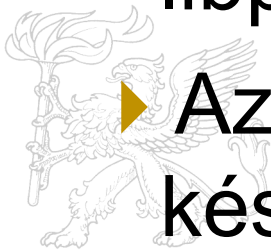
Csomagok megjelölése, ignorálása

- ▶ Megjelölhetünk csomagokat, így a későbbiekben könnyebben megtaláljuk
 - Fekete lesz a háttérszíne a listában
 - Megjelölés: jobb klikk a csomagon, és ott „Mark packet” menüpont
- ▶ Ha ignorálunk egy csomagot, akkor nem tárolódik el sehol – program bezárása után elveszik
 - Fehér háttér, szürke betű, <Ignored> jelölés



Dump

- ▶ Az elfogott csomagok fájlba írhatóak
 - Az ignorált csomagok nem kerülnek bele
- ▶ Létrejön egy .pcap fájl (*WinPcap*)
- ▶ A pcap library segítségével a nyers csomagadatok időbélyeggel ellátva egy libpcap fájlba íródnak
- ▶ Az elmentett eredmény visszatölthető később



Adatok egyesítése

- ▶ A mentett fájlokat össze is fűzhetjük
 - Pl. File → Merge menüvel
 - Több fájl ráhúzása a munkaterületre



Csomag adatainak másolása

1. Jobb egérgomb a csomagon → Copy → Bytes → ... as Printable Text
2. Jobb egérgomb a csomagon → Copy → Summary (Text)

