6. Laborgyakorlat

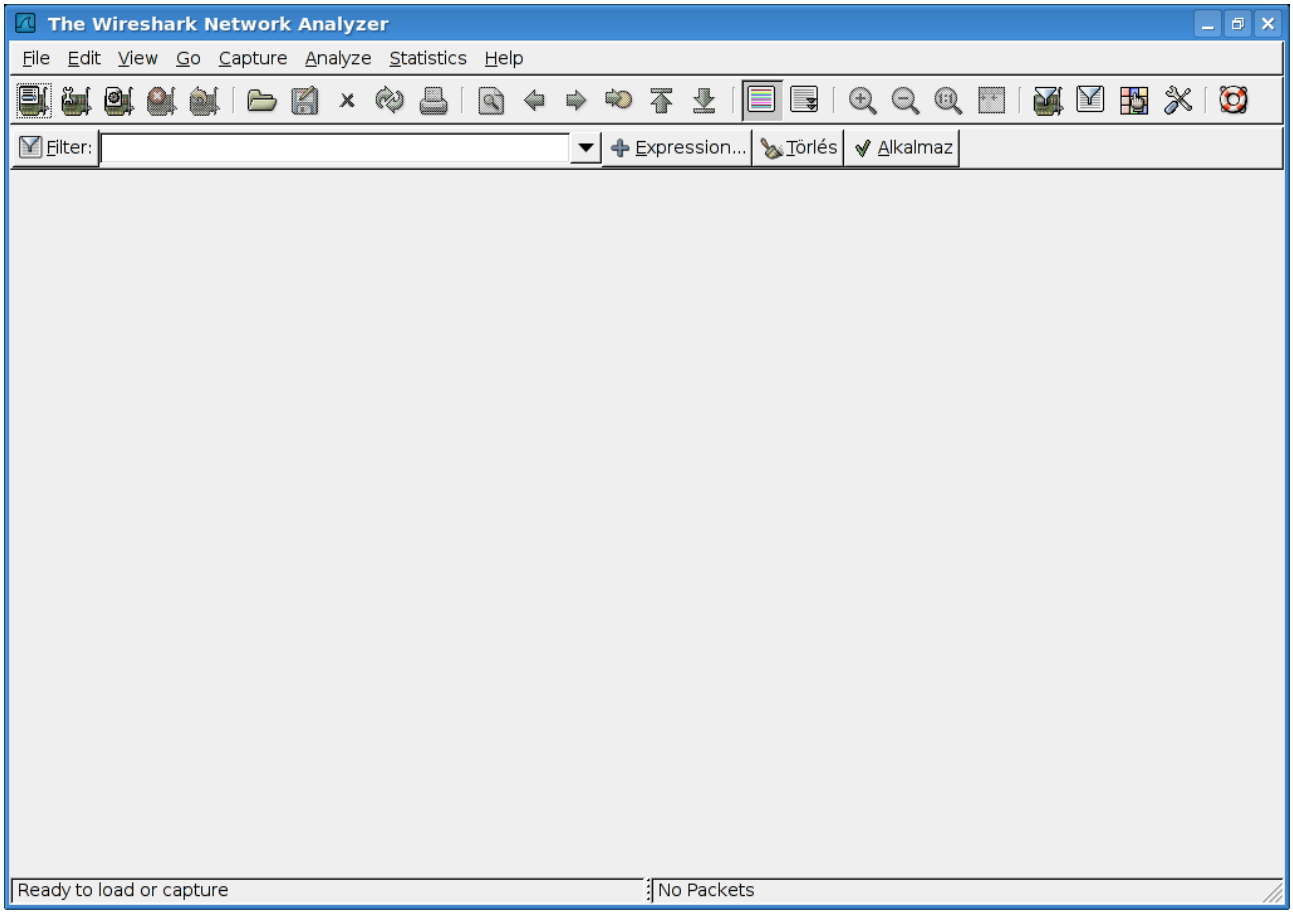
Protokollanalizátor

Néha előfordulhat, hogy a számítógép által elküldött csomagokat vizsgálnunk kell. Ilyen eset lehet például mikor hálózat terhelést vizsgálunk, hogy egy honlap lekérés milyen „mellékes” forgalommal jár (DNS feloldás, reklámok mely szerverekről jönnek). Vagy vizsgálni szeretnénk, hogy egy bizonyos csomagból időegység alatt mennyi fordul elő a hálózaton. Ilyen esetekben protokollanalizátort használunk.

Laborunkban található két „hardveres” protokollanalizátor, a Wandel 10Mbit/sec-es valamint a HP-Agilent 10/100Mbit/sec-es analizátorok. A hardveres protokollanalizátorok, nagyon költségesek, és frissítésük hosszadalmas, egy átlagos felhasználó számára hozzáférhetetlen. A Számítógép-hálózatok tárgy keretében ezért nem a fenti két analizátort használjuk, hanem egy szoftveres megoldást, melyet mind windows-os mind linux-os munkaállomásokon tudunk használni.

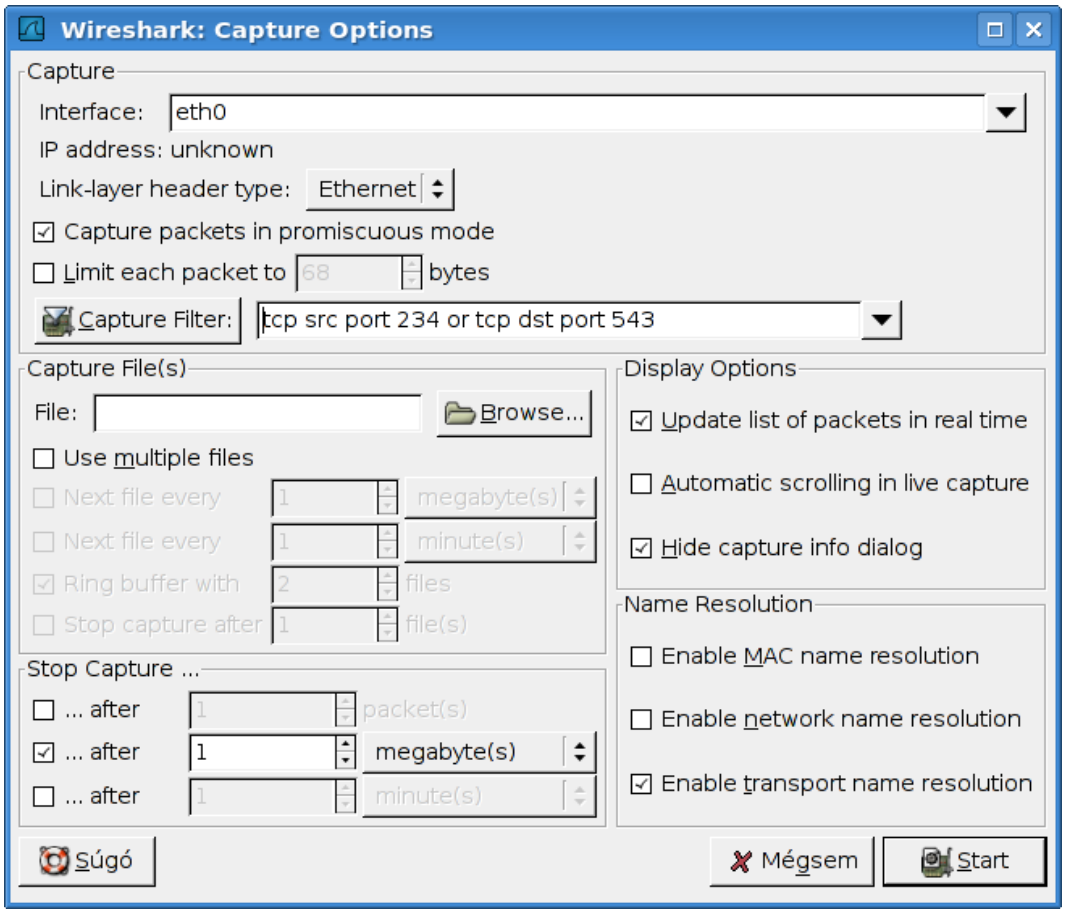
A wireshark egy GNU/GPL licences program. A kezelőfelülete igen egyszerű. Debian GNU/Linux alatt az apt-get install wireshark paranccsal tudjuk telepíteni, windows alá az internetről egy telepítőt kell leszedni, mely a libpcap windowsra fordított telepítőjét is tartalmazza (régebben külön kellett telepíteni).

A program indítás után így néz ki:



Készítette: Sinkó Gergely

A programunk beállításához a 2. ikonra kell kattintanunk, melynek hatására következő beállító ablak fog megnyílni:



A számunkra fontos beállítási lehetőségek:
Interface - az a hálózati kártya melyen a programnak a csomagokat el kell kapnia (ha nem látszik a hálózati kártya a listában a következő parancsot kell kiadnunk: ifconfig eth0 up; ezzel a kártyát „felhúzzuk” de nincs hálózat beállítva)

Stop Capture … - itt állíthatjuk be, hogy mennyi csomagot kapjon el a programunk, megadhatunk csomagszámot, byet-ot, időintervallumot is.

Display Options

Update list of packets in rel time – folyamatosan frissítse az elkapott csomagok listáját

Hide capture info dialog – rejtse el azt az ablakot amelyikben az elkapott csomagok százalékos eloszlását mutatja a program.

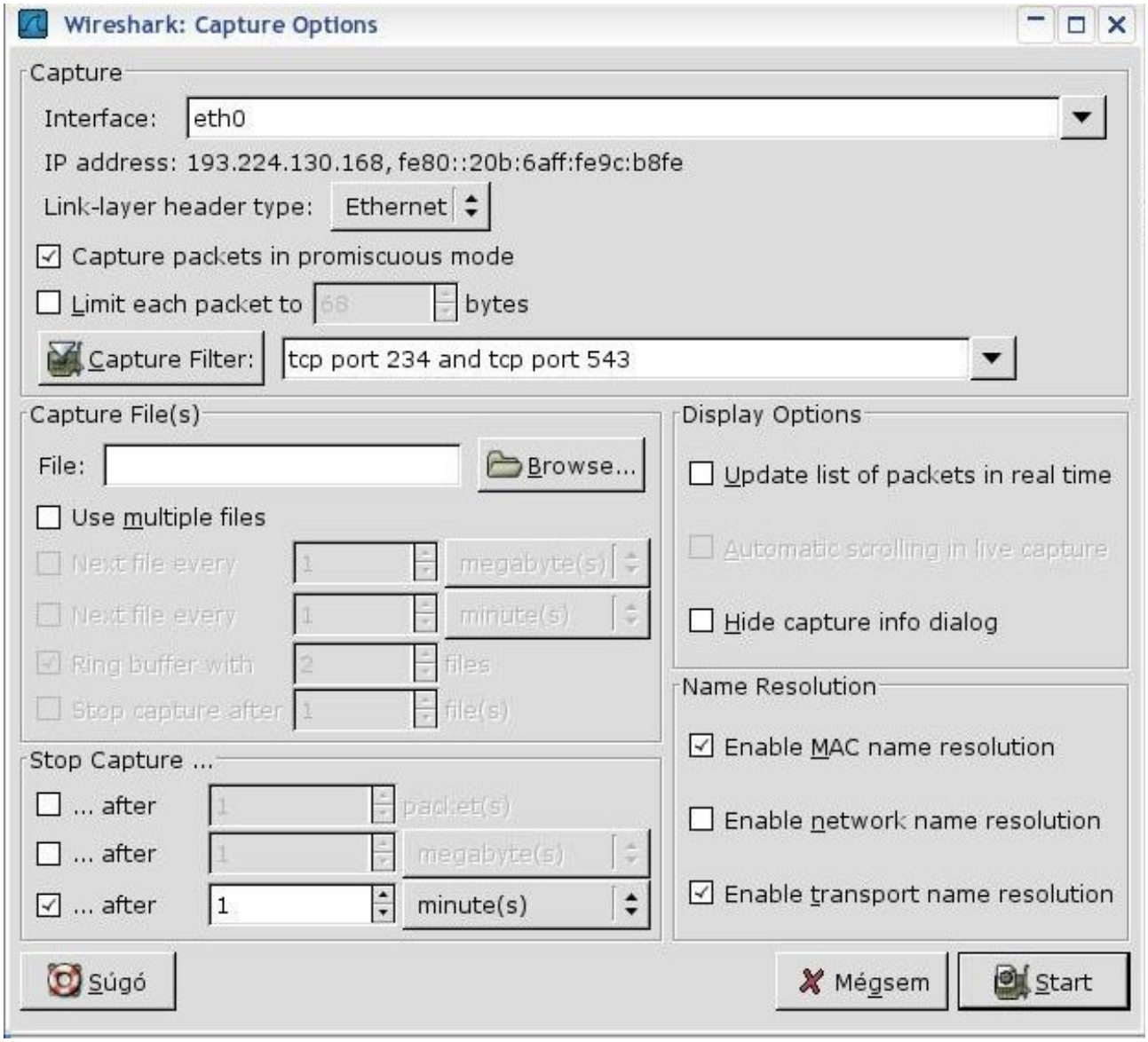
Name Resolution

Enable MAC name resolution – Ezt kikapcsoljuk nincs rá szükségünk, mert felesleges forgalmat generálna

Capture Filter – szűrést állíthatunk be, csak az általunk kért csomagokat kapja el a program, példánkban azokat a TCP csomagokat, melyekben a forrásport 234 vagy a célport 543.

Készítette: Sinkó Gergely

A stop capture - mezőben azt adhatjuk meg, hogy milyen körülmények között állítsa meg a program a csomagok gyűjtését. Itt megadhatunk csomagszámot, időintervallumot, vagy a összméretet.



Készítette: Sinkó Gergely