Wireshark Bevezető

Ez a gyakorlat a Wireshark nevű hálózati forgalomelemző program használatáról fog szólni. Segítségével elkaphatjuk és elemezhetjük a hálózaton közlekedő csomagokat.

A program néhány felhasználási területe:

- hálózati problémák felderítése rendszergazdák számára
- hálózati biztonsági szakembereknek biztonsági rések felderítése
- fejlesztők használhatják a protokoll implementációk tesztelésére, debuggolására
- segítségével megérthető a hálózatok működése
- és még sok más felhasználási terület

A program néhány főbb jellemzője:

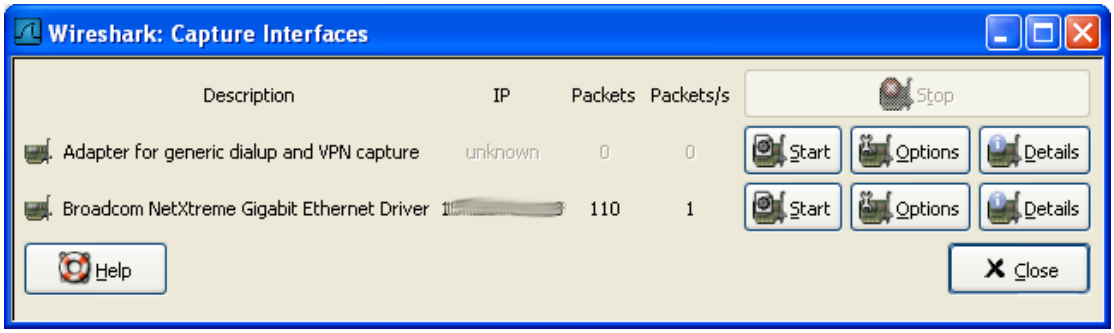
- ingyenesen elérhető (wireshark.org), ugyan itt tutorial is található
- Linuxos és Windowsos verzió is van belőle
- elkapja egy hálózati interfészre érkező adatcsomagokat, ezekről részletes információt szolgáltat
- korlátozható az elfogni kívánt, illetve elfogás után a megjelenített csomagok köre
- a csomagok kereshetők több módon
- a forgalmi adatok elmenthetők és betölthetők

És végül: mire nem jó a Wireshark?

- Nem akadályozza meg, illetve nem figyelmeztet külső behatolás esetén. Ennek ellenére, felhasználhatók a “különös” dolgok felderítésére.
- Nem lehet vele manipulálni a hálózatot, hanem csak mérni, megfigyelni lehet azt.

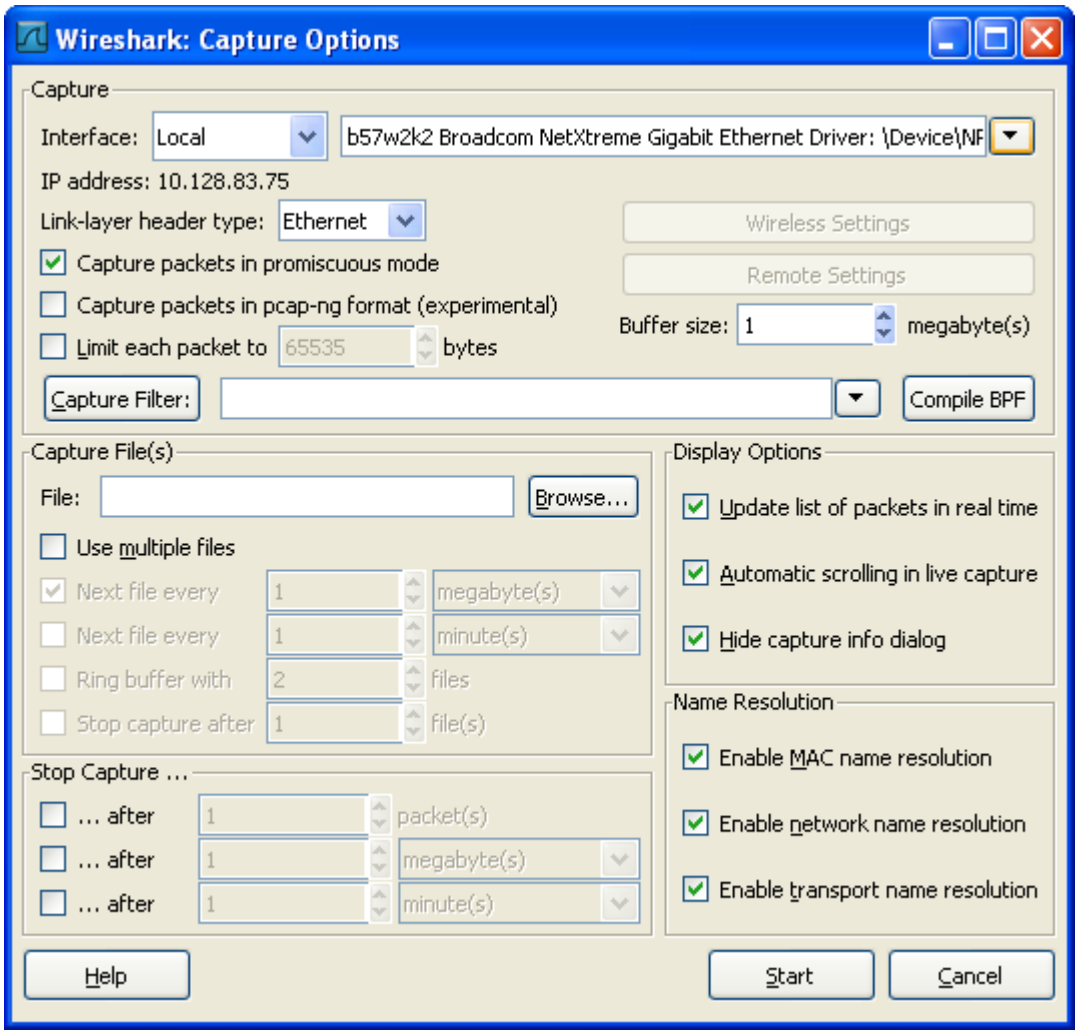
Wireshark

A mérés indításához a “Capture” menü “Interfaces…” menüpontjára kell kattintani (az eszköztáron balról az első ikon). Ekkor a felugró ablakban láthatjuk az elérhető hálózati interfészeket, amiknek a forgalmát figyelhetjük.



1. ábra Interfész választó ablak

Ha megfelelnek az alapértelmezett beállítások, akkor a “Start” gombra kattintva azonnal indíthatjuk a mérést. Hogy melyik interfészre van szükségünk, az IP címe alapján tudjuk eldönteni (az 1. ábrán a második kell nekünk). Az „Options” gombra kattintva beállíthatjuk a mérés paramétereit.



2. ábra Beállítások

Itt most csak egy-két érdekesebb beállítást fogunk megnézni, de a teljes leírás megtalálható a hivatalos tutorialban (http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureOptions.html).

Az első ilyen beállítási lehetőség a „Capture packets in promiscuous mode" jelölőnégyzet. Alaphelyzetben a program csak a saját számítógépünknek címzett csomagokat fogja el. Ha bekapcsoljuk ezt a módot (tehát kipipáljuk a jelölőnégyzetet), akkor minden, a hálózati adapteren átfolyó csomagot elkapunk, nem csak ami nekünk jön.

A „Capture filter" felirat melletti sorba adhatunk meg elfogási szűrőt.

Elfogási szűrők (Capture filter)

Ezek a szűrők arra jók, hogy leszűkítsük az elfogott csomagok körét. A szűrők általános alakja:

[not] **primitive** [and|or [not] **primitive** ...]

A szűrő alap esetben egy primitívből, vagy több primitív éssel vagy vaggyal történő összekapcsolásából áll. Az egyes primitíveket negálhatjuk is a „not" szóval.

Néhány ilyen primitív:

- tcp port <portszám>
- host <hostszám>

További primitívek:
http://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html#ChCapExFilt2

Példa:

A telnet port (23) forgalmának elfogása:
tcp port 23

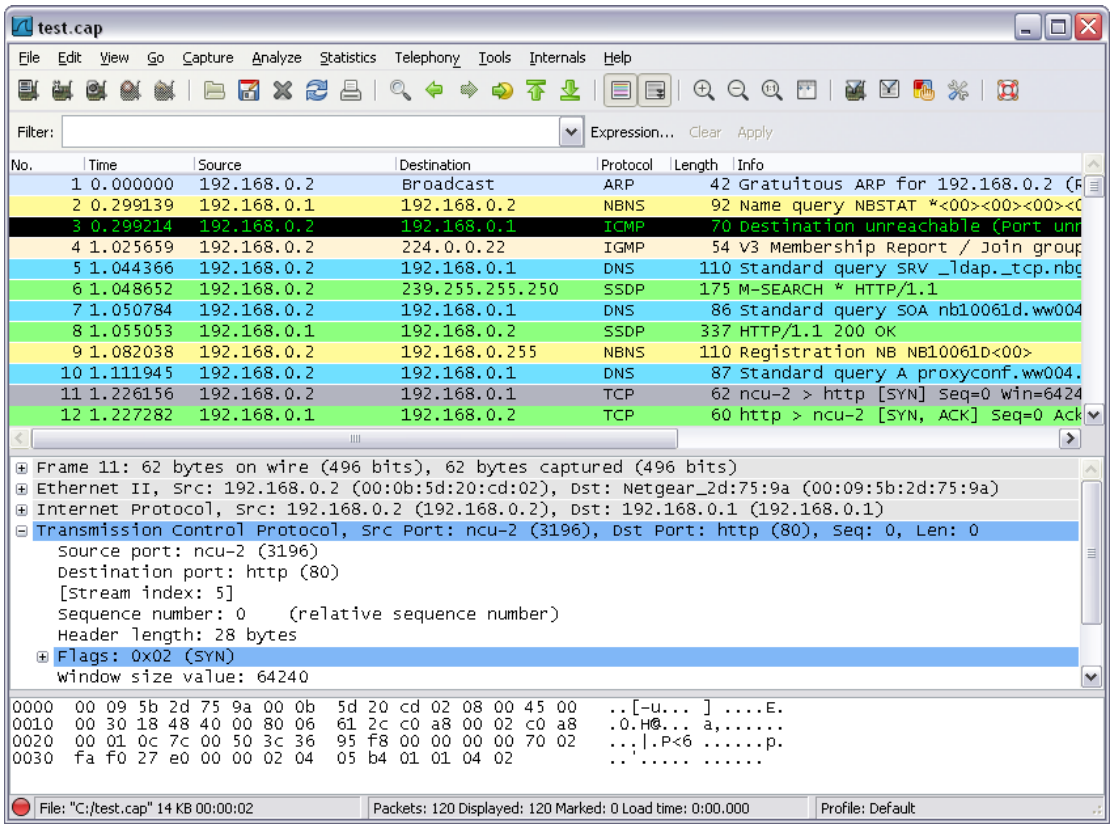
Csak a 10.0.0.5 IP címre/címről érkező telnet csomagokat fogja el:
tcp port 23 and host 10.0.0.5

További példák:

http://wiki.wireshark.org/CaptureFilters

Munka az elfogott csomagokkal

Beállítás után a „Start" gombra kattintva elindul a forgalom figyelése. A listában valós időben jelennek meg az elkapott csomagok.



3. ábra Csomagok listája

A listában látható a csomagok legfőbb adatai: az elkapás ideje, sorszáma (ezzel tudunk rájuk hivatkozni), feladó és fogadó IP címe, a protokoll típusa és egyéb információ. Ha rákattintunk egy csomagra, alul megjelennek a részletes információi (dupla kattintás után új ablakban).

Bizonyos helyekre (fejléc, csomag a listában, részletes nézet) jobb egérgombbal kattintva helyi felugró menüt hozhatunk elő. A helyi menükben található menüpontok részletes leírásait a http://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayPopUpSection.html oldalon olvashatjátok. Ezek közül néhányat emelek ki (de a többi is hasznos).

Fejlécre kattintva:

- Sort Ascending/Sort Descending: rendezi a csomagokat az adott mező szerint növekvő/csökkenő sorrendbe

A listában egy csomagra kattintva:

- **Apply as Filter:** a kiválasztott csomag alapján szűrőt hoz létre és azt alkalmazza a listára
- **Follow TCP Stream:** megjeleníti egy csomópont pár közötti TCP forgalmat

A részletes nézeten kattintva:

- **Wiki Protocol Page:** megnyitja a böngészőben az adott protokoll leírását
- **Filter Field Reference:** az adott protokoll szűrőjének referenciáját nyitja meg a böngészőben

Megjelenítési szűrők (Display filters)

Az elfogott és kilistázott csomagokat tovább szűrhetjük. A szűrőfeltételnek nem megfelelő csomagok nem tűnnek el a listából, csak nem lesznek láthatóak. Szűrhetünk egy adott mező meglétére, mező értékére, protokollra…

Néhány példa szűrőkre:

- egy adott IP címre/ről jövő csomagok

  ip.addr==192.168.0.1
- 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

Szűrőprimitívek: http://www.wireshark.org/docs/dfref/

Szűrőkifejezések létrehozása, tárolása

Ha még nem vagyunk gyakorlottak a szűrőkifejezések létrehozásában, vagy egy adott protokollra vonatkozó primitívekben, akkor segítségünkre lehet a „Filter Expression" dialógusablak. Ez a „Analyze" menüpont, azon belül „Display filters…" menüpontból érhető el. Itt láthatók a már korábban létrehozott szűrők (van néhány alapból). Az „Expression…" gombra kattintva kapunk egy listát, ahol protokollok szerint rendezve megtaláljuk az összes primitívet valamint relációt. Ezek segítségével könnyen összeállíthatjuk a saját szűrőkifejezésünket. Ha nevet is adunk neki, akkor később újra felhasználhatjuk.

Csomagok keresése

Lehetőségünk van egy adott csomag megkeresésére. Erre az „Edit" menü „Find packet…" menüpont (vagy a kis nagyító ikon az eszköztáron) szolgál. Kereshetünk szűrő alapján, byte szekvenciára vagy szövegrészre.

Csomagok megjelölése, ignorálása

A csomagok listájában megjelölhetünk, ignorálhatunk egyes csomagokat. Ezt úgy tehetjük meg, hogy a kívánt csomagra jobb gombbal kattintunk, és ott a Mark packet (jelölés) vagy Ignore packet (ignorálás) menüt választjuk.

Megjelöléskor fekete háttérszínt kap a csomag, így később könnyebb lesz megtalálni.

Ignoráláskor fehér háttérre és szürke betűszínre vált a csomag. Az ignorált csomagok nem kerülnek mentésre, tehát a program bezárása után ez elveszik.

Adatok mentése, betöltése

Lehetőségünk van korábban elfogott adatok betöltésére, illetve az aktuális forgalom elmentésére (ekkor az ignorált csomagok nem mentődnek). Össze is fűzhetünk több fájlt (például, mikor különböző interfészről gyűjtünk adatokat), ezt a „File” menü „Merge” menüpontjával tehetjük meg.

Egyszerűbb mód, ha a kívánt fájlokat egyszerre ráhúzzuk a munkaterületre.