Tavasz | 2017

UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
UNIVERSITY OF SZEGED
Department of Software Engineering

Számítógép-hálózatok 12. gyakorlat
Forgalomfigyelés, Wireshark

Bordé Sándor

Tartalmojegyzék

Bevezetés

Ez a gyakorlat a Wireshark nevű hálózati forgalom figyelő program használatáról fog szólni. Segítségével elkaphatjuk és elemezhetjük a hálózaton közlekedő csomagokat. (Hasonlóan a Packet Tracer szimulációs módjához.)

Kiknek és miben segíthet a program?

- **rendszergazdák**nak a hálózati problémák felderítésében
- **hálózat-biztonsági szakemberek**nek a biztonsági rések felderítése
- **fejlesztők**nek a protokoll implementációk tesztelésénél, debuggolásnál
- **hallgatók**nak a hálózatok működésének megértésében (pl. ez a kurzus)

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

Elméleti hátter

Mivel a program segítségével a hálózaton közlekedő csomagokat lehet elkapni és megvizsgálni, érdemes megismerkedni az ehhez kapcsolódó fogalmakkal. Az OSI modellről és az IP protokollról már volt szó, úgyhogy itt most csak ismétlésként szerepel, a TCP pedig előadáson került elő.

OSI model

A modell a különböző protokollok által nyújtott funkciókat egy rendszerbe szervezi. Jellemzője, hogy minden régete csak a közvetlenül felette lévő rétegnek adhat és csak a közvetlenül alatta lévőtől kérhet szolgáltatást. Az egyes rétegek megvalósíthatók szoftveresen, hardveresen vagy a kettő keverékeként. A szabvány lehetővé teszi, hogy a más gyártók által készített hardverek és szoftverek gondtalanul együttműködhessenek, feltéve, ha követik az előírásokat.

Bővebben: http://hu.wikipedia.org/wiki/OSI_modell

Angolul: http://en.wikipedia.org/wiki/OSI_model

IP (Internet Protocol)

A legismertebb protokoll a hálózati rétegben. Az IP a szállítási rétegtől kapott adatokat datagramokra bontja. Egy datagram egy fej- és egy szövegrészből áll. A fejrészben eltárolásra kerül a küldő és a címzett számítógép IP címe is.

Bővebben: http://hu.wikipedia.org/wiki/IP

Angolul: http://en.wikipedia.org/wiki/Internet_Protocol

TCP (Transmission Control Protocol)

A TCP a szállítási réteg protocolja (4. az OSI modellben). A számítógépes hálózatokon működő alkalmazások többségének megbízható átvitelre van szüksége. Az IP által továbbított datagramok elveszhetnek a hálózaton, esetleg módosulhatnak (best effort továbbítás). A TCP protokoll feladata az adatok hibátlan, helyes sorrendű, hiánytalan és duplikátumok nélkül való továbbítása. Képes az elveszett csomagokat újraküldeni, a helytelen sorrendet pedig visszarendezni. A TCP az adatokat szegmensek formájában továbbítja.

Bővebben: http://hu.wikipedia.org/wiki/Transmission_Control_Protocol

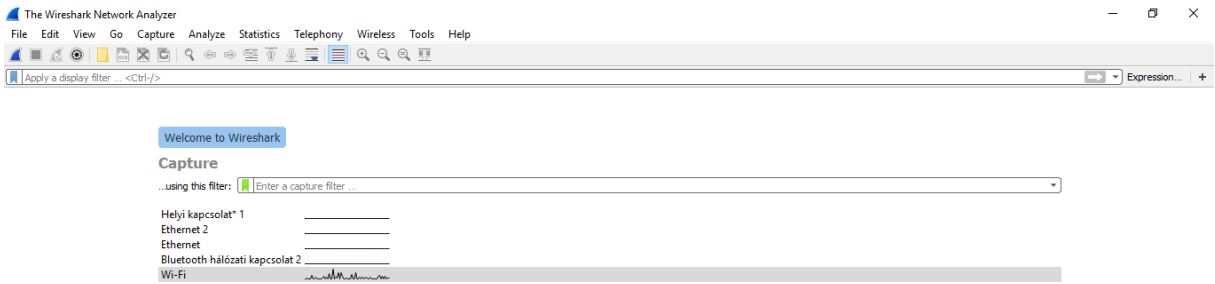
Angolul: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Ismertebb portszámok

- 7 echo
- 21 FTP
- 22 SSH
- 23 TELNET
- 25 SMTP
- 53 DNS
- 80 HTTP
- 110 POP3
- 143 IMAP
- 443 HTTPS

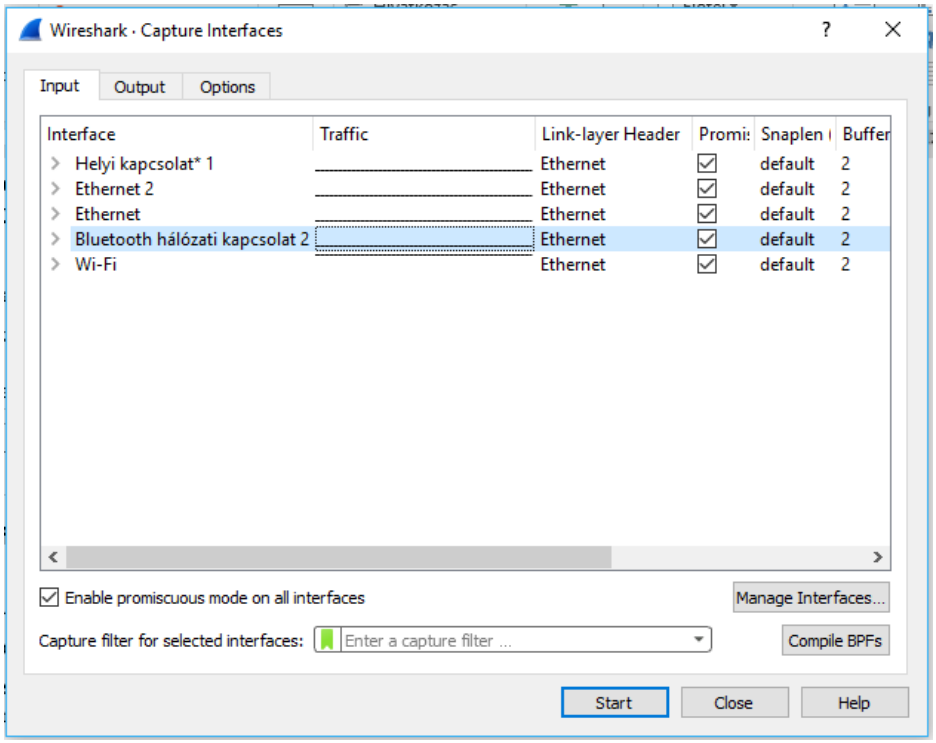
Gyakorlati háttér

A program elindításakor láthatjuk az elérhető hálózati interfészeket, amiknek a forgalmát figyelhetjük. Hogy melyik interfészre van szükségünk, az IP címe alapján tudjuk eldönteni (az 1. ábrán a negyedik kell nekünk).



1. ábra Interfész választó felület

Ha megfelelnek az alapértelmezett beállítások, akkor kétszer az interfészre (vagy egyszer a menüsorban a kék háromszögre – cápauszony) kattintva azonnal indíthatjuk a mérést. Az „Capture options” gombra kattintva (menüsoron a kis fogaskerék) beállíthatjuk a mérés paramétereit. Itt most csak egy-két érdekesebb beállítást fogunk megnézni, de a teljes leírás megtalálható a hivatalos tutorialban.



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 for selected interfaces*” 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 **ÉS**-sel vagy **VAGY**-gyal történő összekapcsolásából áll. Az egyes primitíveket negálhatjuk is a „**not**” szóval.

Néhány ilyen primitív:

- tcp port <portszám>
- host <hostszám>

További primitívek.

Példa:

A telnet port (23) forgalmának elfogása:

```
tcp port 23
```

Csak a 10.0.0.5 IP címre/címről érkező telnet csomagokat fogja el:

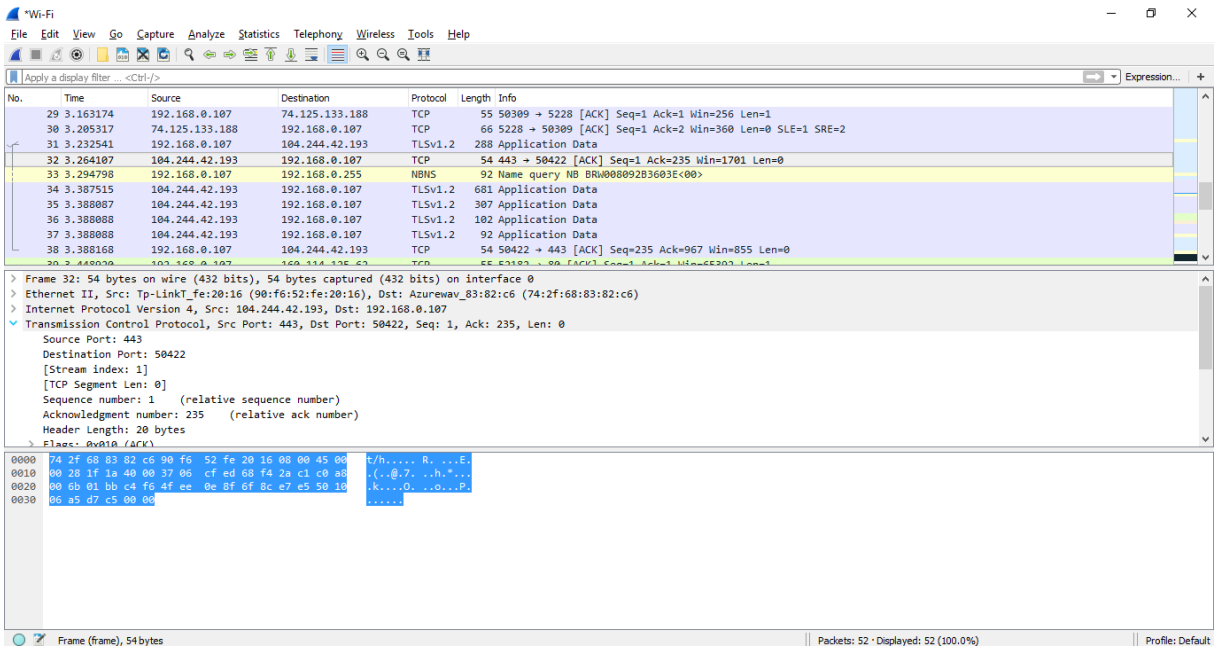
```
tcp port 23 and host 10.0.0.5
```

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.



2. 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 átkerül új ablakba).

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. A csomaglistánk felett lévő, „*Expression…*” gombra kattintva kapunk egy listát, ahol protokollok szerint rendezve megtaláljuk az összes primitívet és 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 „üres” 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 hátterre 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.

Beugró kérdések

- Az alábbiak közül melyik a Wireshark előnye?
- A Wireshark mire nem alkalmas?
- Az OSI modell szerint melyik rétegbe tartozik az IP (Internet Protocol)?
- Az OSI modell szerint melyik rétegbe tartozik a TCP (Transmission Control Protocol)?
- Melyik a HTTP portszáma?
- Melyik kifejezéssel (capture filter) szűrhetünk csak az FTP (21 es port) forgalomra?
- Melyik kifejezéssel (capture filter) szűrhetünk csak a 192.168.2.133 hostról és hostra érkező csomokra?
- Melyik megjelenítési szűrővel (display filter) szűrhetünk csak a POP3 (110-es port) prtokoll forgalmára?
- Melyik megjelenítési szűrővel (display filter) szűrhetünk csak a 127.0.0.1 hostról érkező forgalomra?
- Hogy lehet ignorálni egy csomagot a listában?