SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

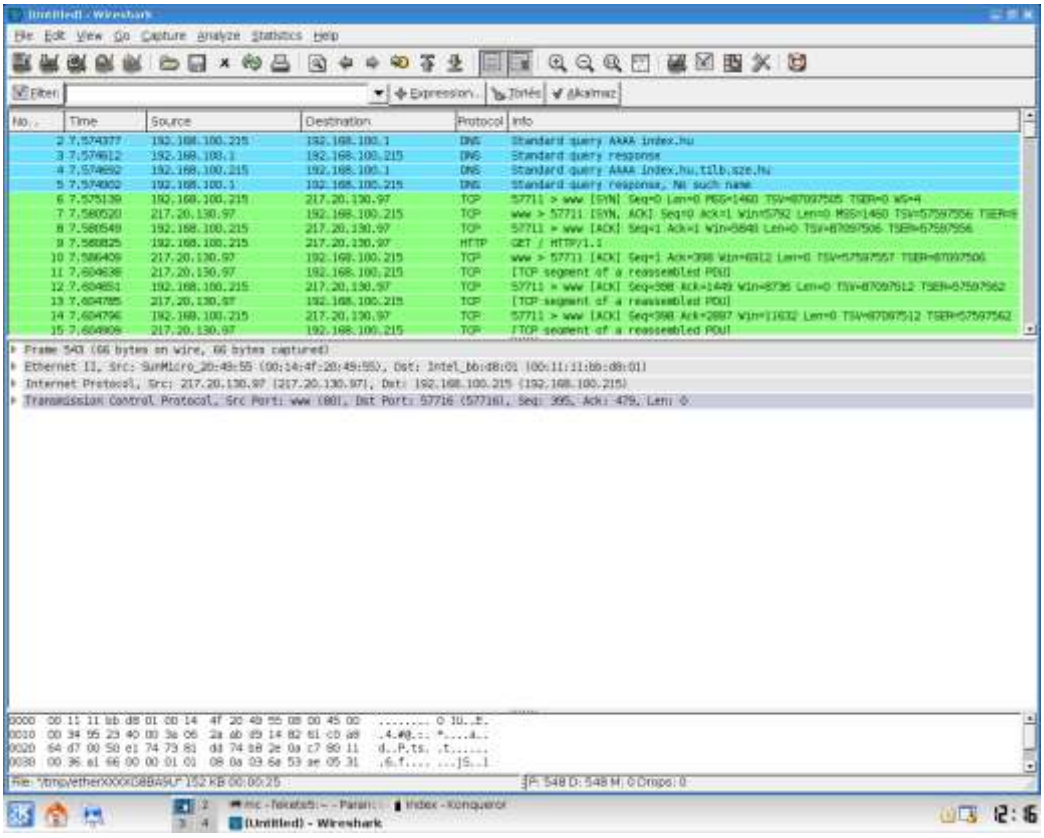
Mérési utasítás TCP: kapcsolat felépítése/bontása, torlódásvezérlés

Előző alkalommal megismerkedtünk a WireShark használatával. Példaként TCP kacsolatok eseteit is használtuk. Ma – a WireShark használatának további gyakorlása mellett – a TCP kapcsolatok elemzésére összpontosítunk.

Kezdjük két ujjgyakorlattal ismétlésként ((1-2) feladat)!

1. **Feladat.**

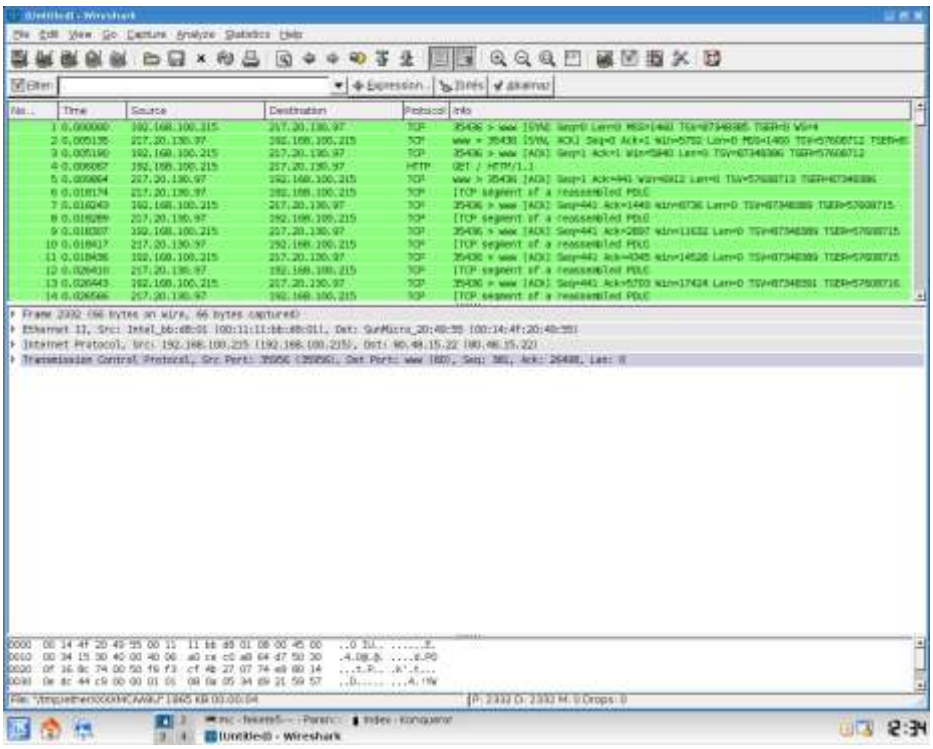
Indítson egy csomagelkapást az eth0-án, úgy hogy a leállítás feltétele legyen 1 perc, valamint a képernyő automatikusan gördüljön a csomagokkal. (Nem kell menteni az előző listát, amennyiben a WireShark megkérdezné.) Ezután a böngészőt elindítva kérje le az *index.hu* honlapot.



Figyeljük meg, hogyan jeleníti meg a WireShark a forrás és cél IP-t, a protokoll nevét, a csomag méretét, az Ethernet opciókat, a forrás és cél MAC címet, valamint a TCP tulajdonságokat: a forrás és cél portot, és a különböző TCP bitek értékét

2. Feladat.

Hajtsa végre az előző feladatot, úgy hogy most filterként beállítva, csak a 80-as portot érintő kommunikációt vizsgálja. (*Capture Filter port 80*).

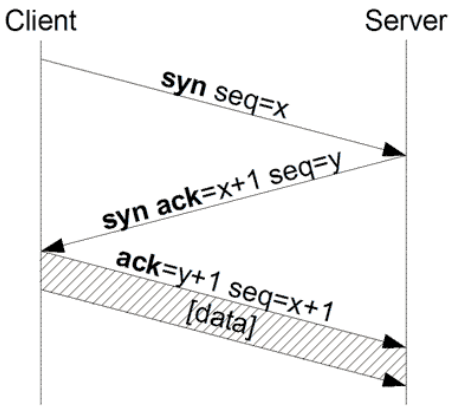


Válasszon ki, bontson ki és figyeljen meg TCP csomagokat.

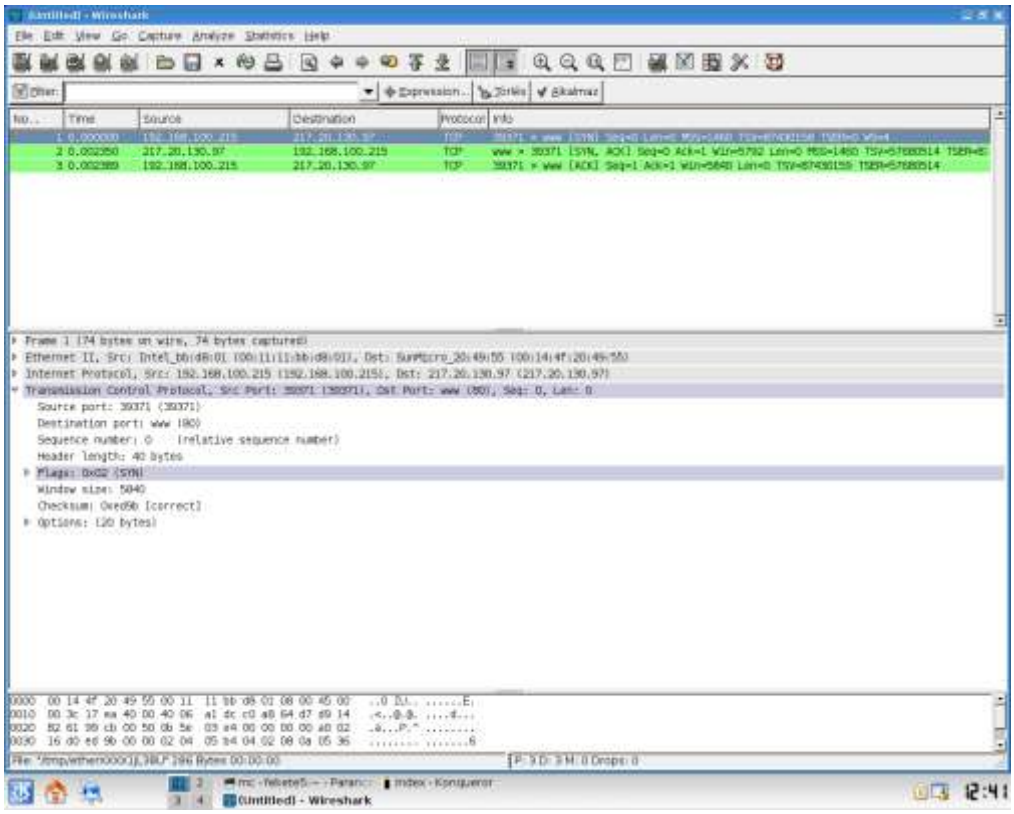
3. Feladat.

Hajtsa végre az előző feladatot úgy, hogy a csomagelkapás leállításának feltétele 3 csomag elkapása legyen. Ezzel az előző feladatból csak a „three-way-handshake”, vagyis a 3 utas kézfogást kapjuk meg.

Ez a TCP protokoll kapcsolat-felépítési fázisa.



SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

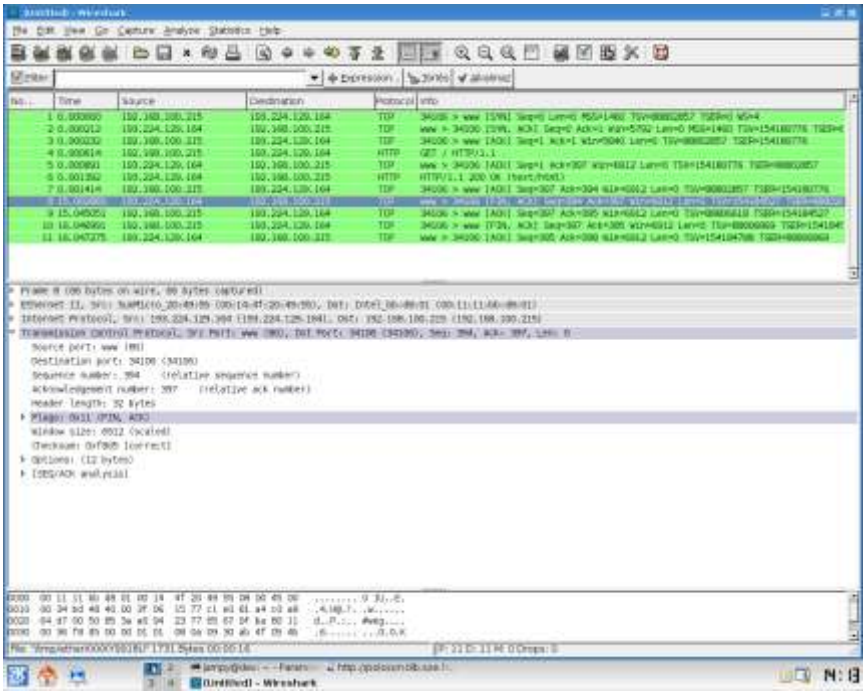


A csomagokat „kibontva” látható, hogy a 3 utas kézfogás egy TCP SYN-nel kezdődik, sequence number=0-val, majd a szerver visszaküldi a TCP SYN,ACK-t , egy sequence number=0 és Acknowledge number=1-el, amelyre a válasz egy TCP ACK, ahol mind a sequence number mind az acknowledge number 1-re van állítva.

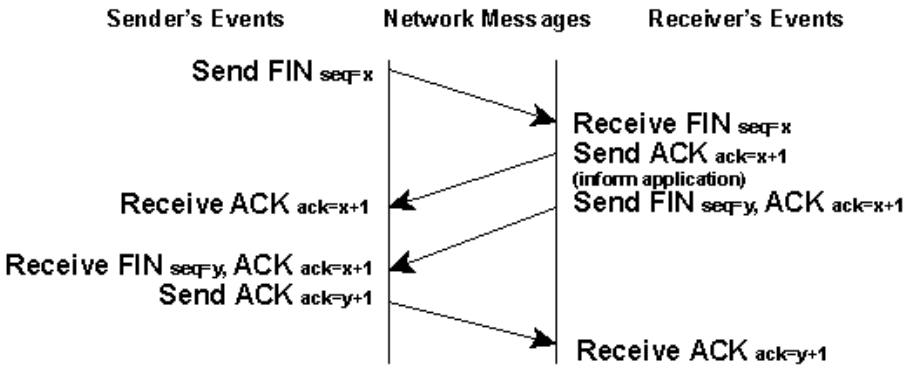
Elevenítse fel a TCP torlódás-vezérléről tanultakat! Végezzen megfigyeléseket a TCP ben az Explicit Congestion Notificationről, ill. az RTT (Round-Trip Time)-ról!

4. Feladat.

Hajtsa végre az előző feladatot úgy, hogy vegye ki a csomagelkapás leállítási feltételt, és most – az egyszerűség kedvéért – a http://dev.tilb.sze.hu lapot kérje le!



Itt az utolsó négy csomagban megfigyelhető a 4 utas kézfogás, mely a TCP kapcsolat lebontását jelenti. Először a szerver küld egy FIN bitet, amelyre ACK a válasz, majd megy egy FIN, amelyre a szerver válaszol ACK-val.



Tegyen megállapításokat az ECN és RTT értékekről!