Beágyazott rendszerek illesztése információs rendszerekhez BMEVIMIM343

dr. Kovácsházy Tamás

Protokoll analizátorok

Méréstechnika és
Információs Rendszerek
Tanszék

Ethernet és TCP/IP mérőeszközök 1.

- Fizikai réteg vizsgáló eszközök (Cable tester)
  - Összeköttetés vizsgálók
    - Be vannak-e kötve, és jól vannak-e bekötve az érpárok?
  - Kábelezési szabványnak történő megfelelőség vizsgálata
    - Frekvencia és időtartománybeli mérések
- Protokoll analizátorok (Protocol Analyzer) HW vagy SW?
  - A referencia modell különböző rétegeiben képesek vizsgálatokat végezni
  - Kérdés, hogy milyen módon kapcsolódunk az analizált hálózathoz
  - Megjelenítik, értelmezik és feldolgozzák az információt, általános célú eszközök
    - Hardver és szoftver fejlesztés, rendszertelepítés, hálózati hiba keresés

Ethernet és TCP/IP mérőeszközök 2.

- Forgalom generátorok és nyelők (Traffic generator)
  - Előre megadható paraméterű, reprodukálható forgalmat generálnak
  - Az adás ás vétel megvalósítása is szükséges
  - Paraméterek: forgalom jellege, nagysága, időzítése
    - Teljesítmény, megbízhatóság tesztelésre fejlesztés során
- Hálózati hiba emulátorok (Network Impairment Emulator)
  - Előre megadható paraméterű, reprodukálható hálózatot emulálnak
  - Paraméterek: csomagvesztés módja, késleltetés, késleltetés ingadozás
    - Eszközök és protokollok tesztelése különböző feltételezett, de nehezen előidézhető hálózati körülmények esetén, fejlesztés során

Ethernet és TCP/IP mérőeszközök 2.

- Forgalom generátorok és nyelők (Traffic generator)
  - Előre megadh… forgalmat gen…
  - Az adás ás vét…
  - Paraméterek: …ítése
    - Teljesítmény, … során
- Hálózati hiba emu… Emulator)
  - Előre megadható p… méterű, reprodukálható hálózatot emuláln…
  - Paraméterek: cso… agvesztés módja, késleltetés, késleltetés ingadozás
    - Eszközök és protokollok tesztelése különböző feltételezett, de nehezen előidézhető hálózati körülmények esetén, fejlesztés során

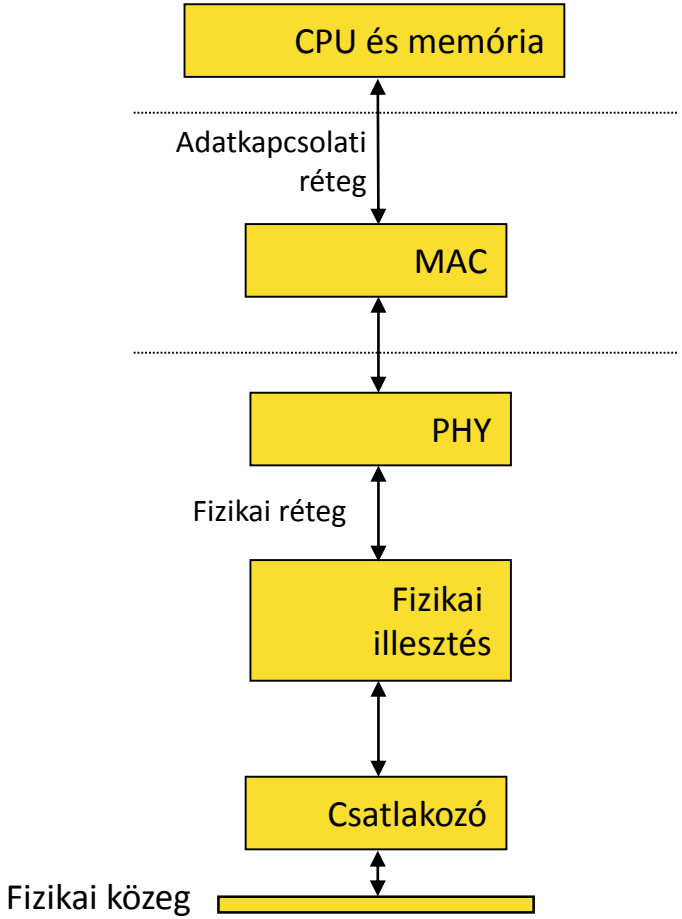
Nem foglalkozunk velük időhiány miatt…

Fizikai réteg vizsgáló (Cable tester)

- Két eszköz a kábel két végén
  - Master és slave eszköz a kábel két végére csatlakoztatva
  - Két ember együttműködése szükséges a méréshez
- Összeköttetés vizsgálók
  - Egyszerű „kicsengetés” érpáronként
  - Hibák pontos megadása valamilyen egyszerű felhasználói felületen
- Szabványosság vizsgálatára alkalmas műszerek
  - Bonyolult frekvenciatartománybeli mérések
    - Frekvenciamenet, Near end echo, Near és Far end crosstalk mérése
    - Időtartománybeli mérések, kábelhossz mérés, Hullám-impedancia, stb.
  - Hiba megadása, hibahely lokalizáció
  - Komplexebb karakteres felhasználói felület vagy GUI
  - Mérési jegyzőkönyv automatikus készítése a gyűjtött adatokból
  - Esetleg optikai mérések támogatása
  - $2000-$10000 USD közötti árak a képességektől függően

Ismétlés: Ethernet rétegek

- Fizikai réteg
  - Bitek/szimbólumok továbbítása
  - A fizikai közegen analóg jelek
  - A kommunikációs hibák ezen a szinten analóg jelek ideálistól eltérését jelentik
- Adatkapcsolati réteg
  - Keretek továbbítása
  - A keret C struktúra jelleggel
  - Esetleg statisztikák az alsóbb rétegekből



HW protokoll analizátorok

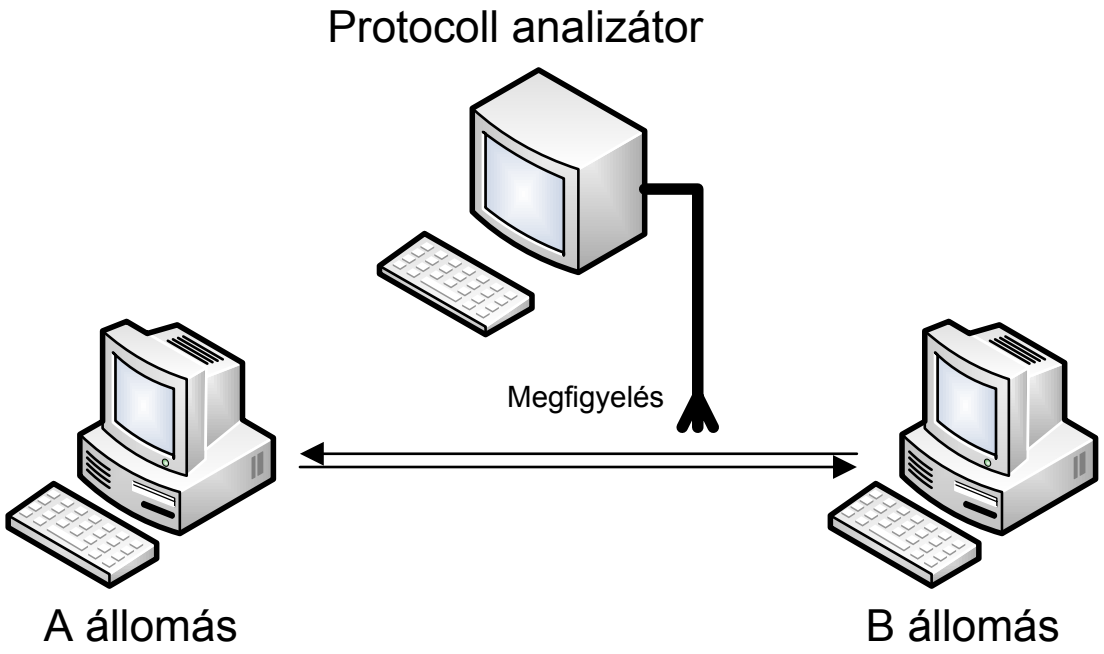
- Fizikai rétegtől működő analizátorok
- Beépített „Ethernet in-service pass-through” vagy külső splitter/tap
- Speciális HW, wire speed, csomagvesztés nem fordulhat elő
- Eye diagramm, fizikai réteg hibák, BER, stb. mérhető
- Analízis az alkalmazási rétegig, intelligens analízis, esetleg forgalom generálás is
- Anritsu, Agilent, stb. speciális mérőeszközök
  - Magas alapár (több tízezer USD-től), rengeteg drága opció
- Megvásárlásuk indokolható az alábbi esetekben:
  - Ilyen eszközöket nagy darabszámban gyártó cég
  - Elsődlegesen ilyen HW-ét fejlesztő cég
  - Ilyen eszközök bevizsgálásával foglalkozó cég
- Minden más esetben bérelni kell, bérbe méretni, stb.
  - Az eszköz gyorsan elavul
  - Kezelésük bonyolult, speciális ismereteket igényel
  - Érdemes megvizsgálni, hogyan megkerülhető-e még a bérlés is…

SW protokoll analizátorok

- Adatkapcsolati rétegtől kezdve képesek működni
  - Nem csak Ethernet estén működnek, WIFI, PPP, stb. kapcsolatokra is működnek bizonyos megkötésekkel
- Forgalom rögzítése:
  - Speciális capture card (pl. DAG card http://www.endace.com/)
    - Built in passthrough (packet copy) vagy külső splitter/tap
    - 100%-os csomagrögzítési garancia a kártya saját memóriájába
    - Néhány ezer USD HW ár (konfigurációtól függ)
    - SW ár ennek a többszöröse
    - IEEE 802.11 (WIFI) esetén pl. AirPcap (http://www.cacetech.com/)
  - Standard Ethernet NIC (dedikált vagy nem dedikált)
    - Csatlakozás a hálózathoz megoldandó
    - Csomagvesztéssel, egyéb hibákkal számolni kell
    - HW ár minimális (a kártya minőségétől sok függ persze)
    - Szoftver: Van szabad forráskodú, ingyenes (WireShark)
    - IEEE 802.11 és Windows esetén driver függő korlátozások

Csatlakozás a rendszerbe

- Két kommunikáló fél esetén
  - Dedikált analizátor esetén lásd ábra
  - A vagy B állomásokon is futhat egy SW analizátor
- Elosztott rendszerben?
  - Alkalmas hely megtalálása
  - Elosztott analizátor



SW analizátor csatlakoztatása 1.

- Splitter (néha hívják tap-nek is)
  - Párban kell használni (adás és vétel ág) és a forgalom rögzítéshez is két eszköz kell (adás ág és vétel ág külön)
  - A beiktatási csillapítással számolni kell
  - Optikai megoldások nagyobb számban elérhetők a piacon
  - Léteznek CAT5/5e megoldások is
    - A legtöbb ilyen az Internet-en fellelhető eszköz a megadott adatok alapján a célra alkalmatlan!
- Ethernet HUB (ismétlő) alkalmazása
  - Beavatkozik a hálózatba fizikai szinten (CSMA/CD)
    - A forgalom jellegétől függ az általa okozott hiba
    - Kis forgalom és rövid kábelek esetén elhanyagolható a hatása
  - Csak 10Base-T vagy 100Base-TX esetén alkalmazható
    - 1000Base-T HUB-ok már nem kerültek piacra
  - Nem gyártják már (ezért jó néhányat a szekrénybe tartalékolni)
  - Egyszerű megoldás beágyazott rendszerek fejlesztése során, ha van néhány a raktárban…

SW analizátor csatlakoztatása 2.

- Ethernet kapcsolón port tükrözés
  - A menedzselhető Ethernet kapcsolókon többnyire beállítható, hogy egy adott port teljes forgalmát egy másikra másolja (port mirroring)
  - Keretvesztés történhet
  - Full duplex forrás forgalma megy a mirror kimenet adás vonalára
    - Szűk keresztmetszet lehet, ha a mirror port nem legalább 2x nagyobb sebességű a másolt portnál
    - Pl. 10/100-as portoknál (beágyazott rendszerekben gyakori) használjunk 1000Base-T portot mirror portnak
    - Gigabites rendszereknél 10GBase portok merülnek fel, itt a SW protokoll analizátorok jelentik a szűk keresztmetszetet (aktív kutatási terület)
  - Időtartománybeli viselkedés is sérül
    - Sorrendiség, késleltetés, késleltetés ingadozás
  - Széles körben használják
    - Hálózati behatolás jelző
    - Statisztikák készítése

SW analizátor csatlakoztatása 3.

- Az analizátor futtatása valamelyik kommunikáló állomáson
  - Ha a kérdéses állomás Windows, Linux, BSD Unix (pl. MAC OS X) operációs rendszereket futtat
    - Ha ilyen komponense van a rendszernek, akkor lehet az
      - Ha azon is elérhető a vizsgálandó forgalom
      - És azon futtatható a GUI is
    - Ez a fejlesztő munkaállomás lehet beágyazott komponensek fejlesztése során
  - OS szintű forgalom rögzítés tulajdonképpen
    - A NIC működésébe is be kell avatkozni bizonyos esetekben
  - Problémák
    - Erőforrásokon osztozik az analizátor a rendszer többi részével
      - Közös CPU és memória
      - Szűk keresztmetszet miatt mérési hibák
      - Csomagvesztés (esetleg jelzéssel) és időmérési pontatlanságok
      - 100 Mb/s sebességig kevés probléma, utána sok…

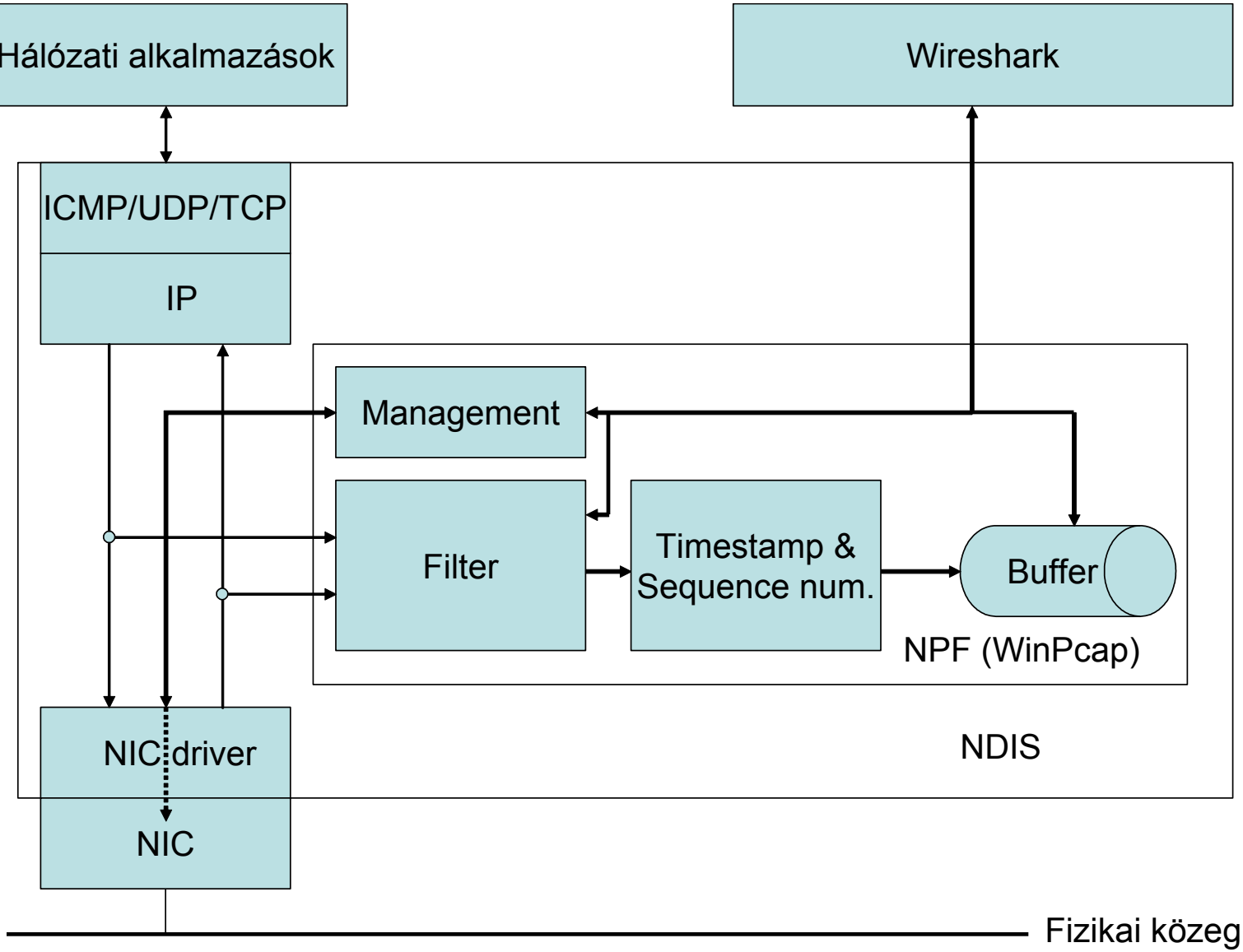
PC alkalmazása SW analizátorként

- Protokoll analizátor szoftver
  - WireShark (http://www.wireshark.org/)
    - Multiplatform: Windows, OS X, Linux, egyéb UNIX variánsok
    - Szabad forráskódú, GNU General Public License version 2
  - Vannak más ingyenes és fizetős szoftverek is
  - A WireShark a legjobb ingyenes szoftver, a legtöbb alkalmazásban elég a tudása
- Hálózati kártyának támogatnia kell
  - WHCL tanúsítvánnyal rendelkező NIC-ek tudják
  - TCP Offload Engine (TOE) megzavarhatja
    - Többnyire a driverben kikapcsolható Windows alatt

Kernel driver

- Kell egy speciális kernel driver
  - UNIX variánsok: libpcap (része a disztribúcióknak)
    - PF_RING és TNAPI (teljesítmény optimalizálás)
  - Windows: winpcap (http://www.winpcap.org/)
- Installálásukhoz root/Rendszergazda jogosultság kell
  - Linux alatt a futtatáshoz is (helyesen)
- Kompatibilitási problémák
  - Bizonyos szerencsétlenül megírt tűzfalakkal nem kompatibilis
  - Bizonyos víruskereső szoftverekkel nem kompatbilis
  - Miért?
    - Ezek a szoftverek szintén beépülnek a protokoll készletbe, sokszor Wireshark elé
    - Az információt nem engedik át, vagy szűrik

Libpcap/winpcap működése



Libpcap/winpcap

- Beépül az OS protokoll készletébe, közvetlen az Ethernet driver fölé
  - Az ilyen jellegű beépülésre az OS-ek lehetőséget adnak
  - Dinamikusan ki- és bekapcsolható az alkalmazásból
  - Hozzáfér a NIC HW konfigurációjához
  - Minden a szűrési feltételnek megfelelő keret duplikál
  - Azokat ellátja időbélyeggel és sorszámmal
  - Egy bufferban tárolja és elérhetővé teszi az alkalmazás számára
  - Teljes tárolás, vagy adott számú byte a keret elejéről
  - Erőforrás igény nagy, szűrés (JIT!), memcpy és kernel-user space váltás (optimalizáció: pf_ring, ntapi)
- Overhead-et okoz
  - A NIC, az OS, és a libpcap/winpcap nyilvántartják, hogy hány keretet küldtek és fogadtak
  - Sajnos a számlálók értékeiben nagyobb hálózati forgalomnál vannak különbségek...

NIC configuráció

- Minden Ethernet kártya tartalmaz egy HW szűrőt
  - Csak a kártya saját címével egyező célcímű beérkező unicast kereteket juttatja el az OS-nek
  - Többnyire van egy multicast filter is
    - Hash alapú, valószínűségi szűrés
    - A gépnek tetszőleges számú multicast címe lehet
  - Ethernet kapcsoló alapú hálózatban már a kapcsoló is szűr (emlékeztető a következő fólián)
- Ezt tetszőleges forgalom rögzítéséhez (nem nekünk szóló forgalom) ki kell kapcsolni
  - A NIC-et „Promiscuous mode” állapotba kell helyezni
  - Promiscuous = mindenkivel meggondolatlanul kapcsolatot teremtő
  - Ezt más SW is használja
    - Pl. SW bridge a VMWARE vagy más virtualizációs megoldásokban

Emlékeztető: Kerettovábbítás hidakban

- A „forwarding database” alapján:
  - Keret beérkezik az ingress porton
  - Adatbázis frissítése a forráscím alapján
  - Továbbítási döntés a célcím alapján:
    - Ismert unicast cím: Az adott unicast címhez tartozó portra kiküldésre kerül, kivéve ha az az ingress port (szűrés)
    - Ismeretlen unicast cím: Minden portra kiküldésre kerül kivéve az ingress port (elárasztás), hátha válaszol rá a kérdéses gép (és akkor meg lehet tanulni)
    - Multicast cím: Alapesetben elárasztás, multicast tanulás esetén minden az adott multicast címre regisztrált portra kiküldésre kerül kivéve az ingress port
    - Broadcast cím: Elárasztás
- Modern hálózatokban nehéz két állomás forgalmát egy harmadikról megfigyelni
  - Éppen ezért került kifejlesztésre a mirror port funkció

Libpcap/winpcap rögzítési szűrő

- Egy egyszerű nyelv szolgál a leírására
  - `([not] primitive [and|or [not] primitive ...])`
  - A megadott szűrőt egy JIT compiler gépi kódra fordítja, és az szűr
  - A WireShark egy GUI-t ad a szűrők megkonstruálására
    - Gyakorlat lesz ezzel kapcsolatban
- Elkerülhetjük a vizsgálat szempontjából nem fontos forgalom rögzítését
  - Kisebb futási erőforrás igény (szűrő gyors)
  - Kisebb tárterület a forgalom tárolására
  - Gyorsabb analízis

Időbélyeg és sorszám

- A szűrési feltételnek megfelelő keretek
  - Időbélyeget és sorszámot kapnak
    - Az időbélyeg forrása?
      - OS nagyfelbontású timer
      - A rögzítés időpontját adja meg, nem a megérkezés időpontját
  - Mindkettő relatív a forgalomrögzítés megkezdéséhez
- Ezeket az információkat a libpcap/winpcap egy pszeudó-fejrészben fűzi a kerethez
  - Rögzített keret az Ethernet fejrésszel kezdődik
  - Elé egy időbélyeget és sorszámot tartalmazó fejrész kerül
  - Ezt kapja meg az alkalmazás és meg is jeleníti
    - Fejrész az Ethernet keret előtt (sokan félreértik)

Rögzített forgalom tárolása

- Megadható méretű kernel buffer
- Megadható, hogy a keret elejéből hány byte kerüljön tárolásra
  - Helytakarékosság (a fejrész elég az analízishez egyes esetekben)
  - Biztonsági megfontolások (érzékeny info. nem kerül be)
- Az alkalmazásba átmozgatva bármit lehet az információval csinálni
  - A mozgatásnak on-line kell történnie
    - Véges kernel buffer
  - On-line analízis: A beérkező keretek azonnal megjelenítésre kerülnek
  - Off-line analízis: A beérkező keretek az alkalmazás memóriájába kerülnek, majd a rögzítés leállítása után analizálhatóak
  - A keretek on-line vagy off-line file-ba menthetők, és a file-ok off-line analizálhatók (több formátum támogatott)

Megjelenítés konfigurálása

- On-line megjelenítés
  - Nem ajánlom a használatát
  - Erőforrás igényes
  - Erősen befolyásolja a rögzítés folyamatát
    - „Mérési hiba” nő
- Off-line megjelenítés
  - Esetleg statisztika megjelenítés (Capture info dialog)
- Preferencies/Capture
  - Minden tiltva kivéve „Capture Packets in Promiscuous mode”
  - Nagy forgalomnál esetleg „Hide capture info dialog” is tiltva
- Preferences/Name resolution
  - Tiltva „Enable network name resolution”, minden más engedélyezve
  - Nagy forgalmat eredményezhet a küldött DNS kérések miatt

A rögzített forgalom megjelenítése

- Megjelenítés
  - Keretekek listája
    - Megadható szabályok szerint színezve
      - Adott szín adott protokollt jelent
      - A színezés konfigurálható
  - A keretlistán kiválasztott keret fejrészenként dekódolva
    - Dissectors
      - Több mint ezer (1034) protokollt ismer az aktuális 1.2.2-es verzió
      - Jól dokumentált módon bővíthető új dissectorral szükség esetén (SW fejlesztés)
    - Ethernet OIU, Ethertype, SNMP MIB, stb. adatbázisok
      - A GUI-n nem csak egy szám jelenik meg
  - Keret ASCII és HEX tartalma

Analízis és statisztikák

- Rengeteg lehetőség
  - Display filter
    - A rögzített forgalomból szabályok alapján kiválasztani az érdekeseket
    - Varázsló segíti a beállítását
    - Sok analízis és statisztika funkció is beállítja
    - Törölni kell, ha mindent látni akarunk
  - Analízis menü
    - Follow TCP/UDP/SSL stream
      - Az éppen kiválasztott kerethez tartozó folyamra konstruál egy szőrőt, és azt beállítja
    - Expert infó
      - A forgalom alapján hálózati problémák felismerése
    - Alapértelmezett decoder (dissector) felüldefiniálása
  - Statisztika menü (majd megnézzük)
  - Telephony menü (VoIP és IPTV stb. specifikus)