Számítógép hálózatok kriminálteknikai vizsgálata

Illési Zsolt CIS[A|M]
informatikai igazságügyi szakértő
illesi.zsolt@proteus.com

Robothadviselés 9
2009. november 24.

Témák

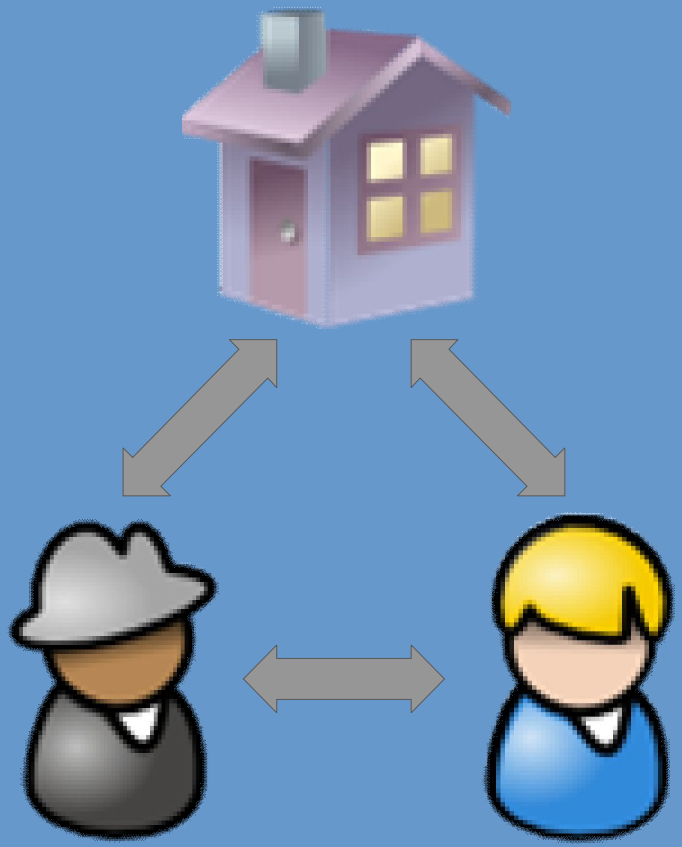
- Igazságügyi szakértés
- Igazságügyi szakértés alapelvei
- Számítógép hálózatok vizsgálati problémái
- Számítógép hálózatok – vizsgálati rétegek
- Nyitott kérdések

Igazságügyi szakértés céljai

- Sajátos szaktudás biztosítása a hatóságok számára
  - bűncselekmények (Btk. és Be)
  - jogviták (Ptk. és Pp.)
- (Bizonyítékszerzés), bizonyítékértékelés, mikrobizonyítás

Locard-féle anyagátadási szabály

- Minden érintkezés nyomot hagy
  - tetthely
  - elkövető
  - áldozat
- Nyom:
  - lenyomat
  - anyagmaradvány
  - adatmaradvány



Számítógép hálózatok és a büntetőeljárás kapcsolata

Számítógép hálózat /hálózati eszköz lehet

- célpont,
- megvalósítási/elkövetési tárgy/környezet,
- elkövetést/megvalósítást megkönnyítő eszköz
- az elkövetés „tanúja”

Számítógép hálózat, mint bizonyítékforrás

A számítógépes hálózatból kinyert bizonyíték

- eredeti/ származékos
- tárgyi jellegű
- terhelő/ mentő
- közvetlen/ közvetett

- Irreverzibilis bizonyítékforrás
  (ex tunc et alicundo)

Daubert kritériumok

A bizonyítás **jogszerű**, ha

- megfelel 1998. évi XIX. tv. a büntetőeljárásról szabályainak

A bizonyítás **szakszerű**, ha

- gyakorlatban is ellenőrzött (tesztelt) elméletre épül
- előzetes bírálat alapján tudományban elismert módon publikált
- ismert a hibaaránya
- a szakemberek tekintélyes közössége által elismert

JPÉ (logika és a józan paraszti ész)

Logikus, ok-okozati érvelés

- ~formális~ logika
- tévedés, következetlenség, manipuláció hatásainak csökkentése
- helyes hangsúly

Occam borotvája

- valamennyi bizonyíték alapján a legegyszerűbb magyarázat a legvalószínűbb

Vizsgálati célok

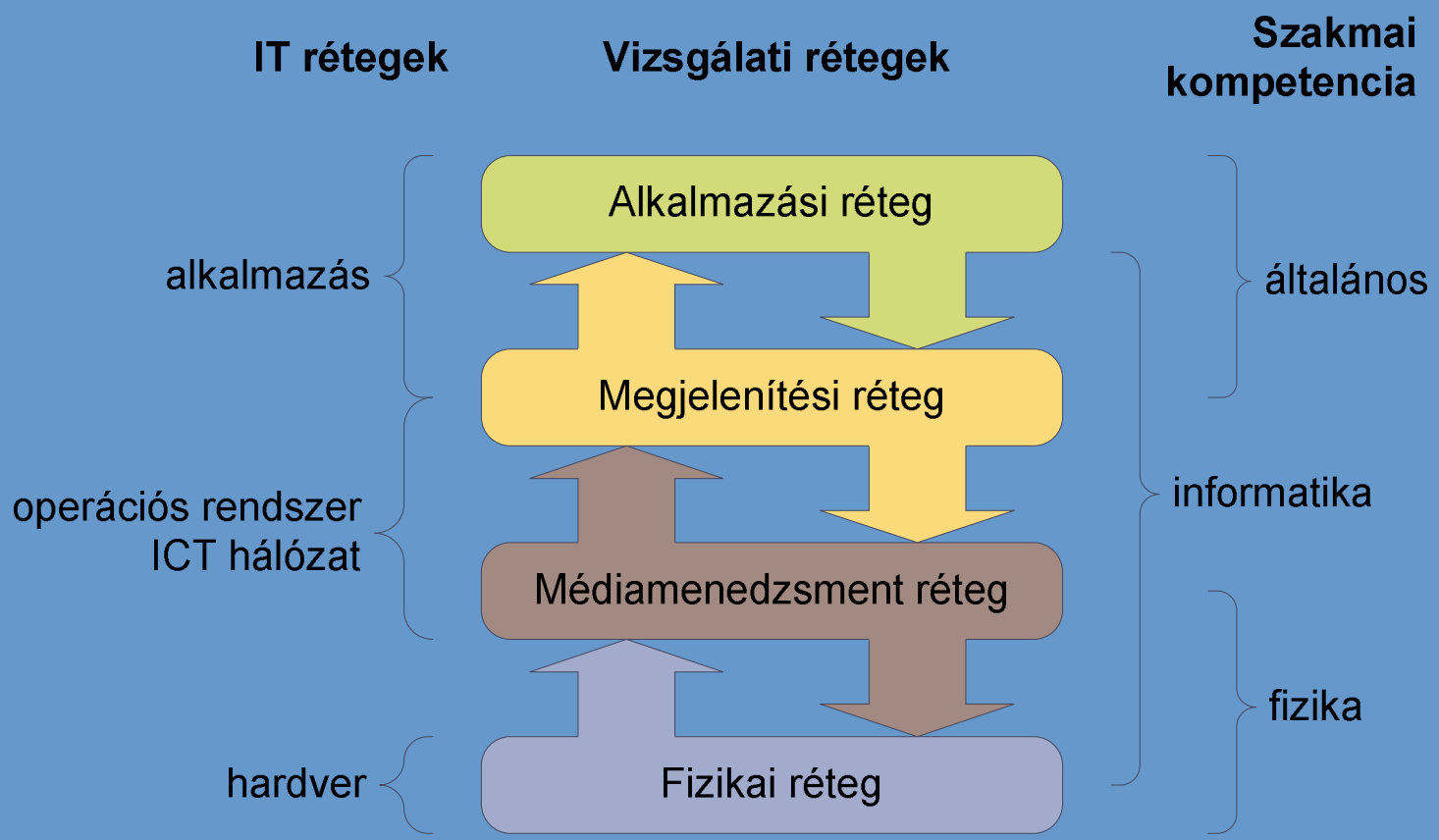
Információgyűjtés a(z)

- elkövető(k)ről (**Ki?**)
- események valós természetével kapcsolatban (**Mit?**)
- események helyszínével kapcsolatban (**Hol?**)
- események sorrendjével kapcsolatban (**Mikor?**)
- motivációs tényezőkkel kapcsolatban (**Miért?**)
- elkövetés módjáról és a felhasznált eszközökről (**Hogyan?**)

Számítógépes hálózat általános felépítése

- hálózat
  - közeg
    - levegő/ vákum
    - réz
    - üveg
  - aktív eszközök
    - ISO/OSI – ICP/IP rétegek támogatása
- végpont
  - szerver
  - munkaállomás
  - aktív eszköz

Informatikai rendszerek vizsgálati rétegei

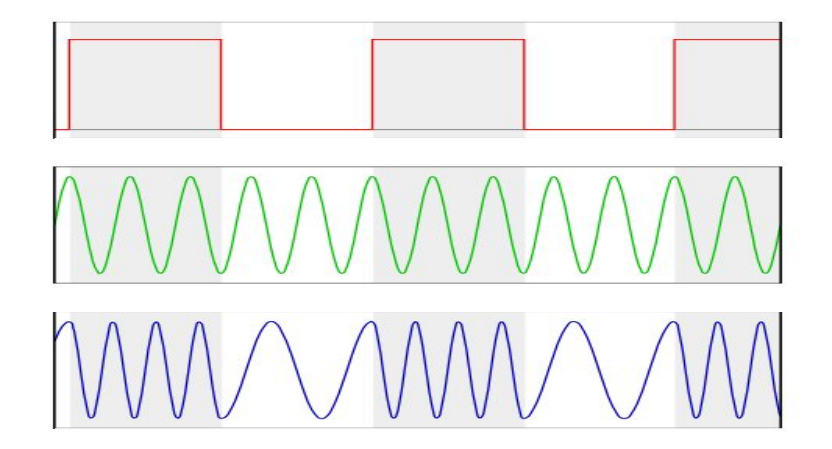


Fizikai réteg

- A csatorna (átviteli és tárolási közeg) fizikai és elektromos specifikációja
  - elektromágneses spektrum
  - kódolás
  - interfész és kábel specifikációk

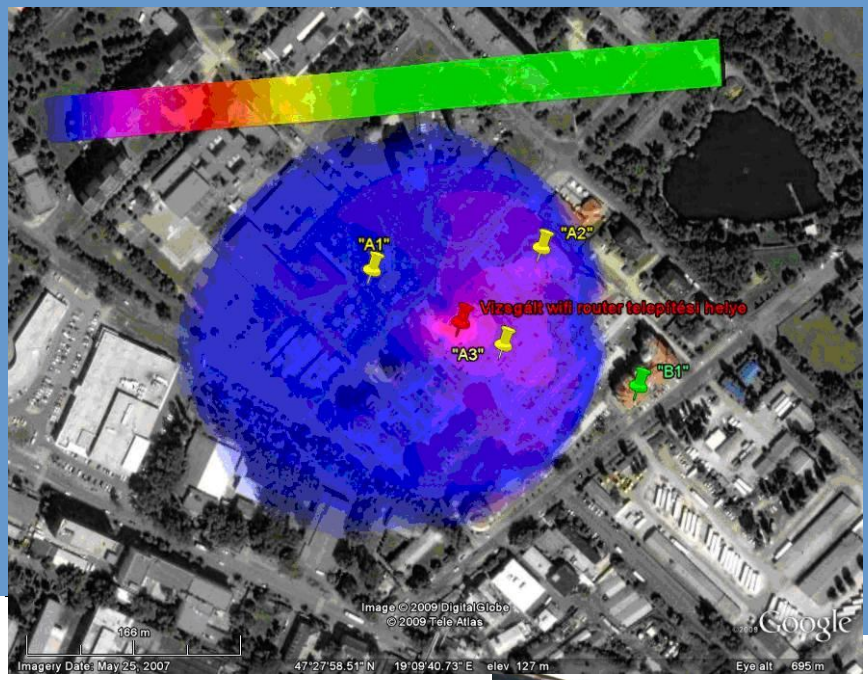
- Módszerek, csatolók, funkciók és eljárások, amelyek lehetővé teszik a hozzáférést az adatokhoz (bit/bájt)

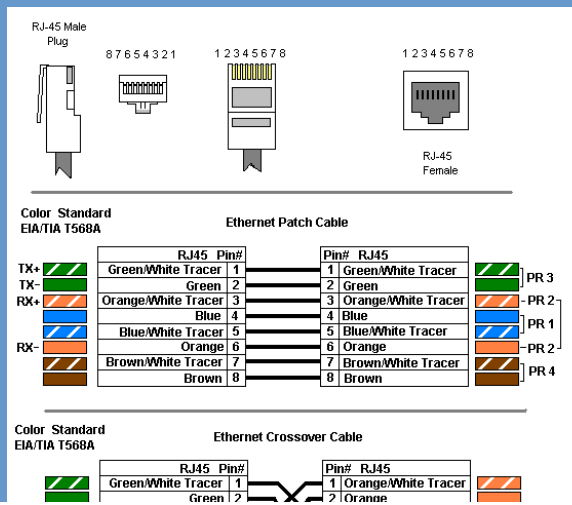
(*Kódolás/ dekódolás? Mi, hogyan és mivel értelmezhető adatként?*)

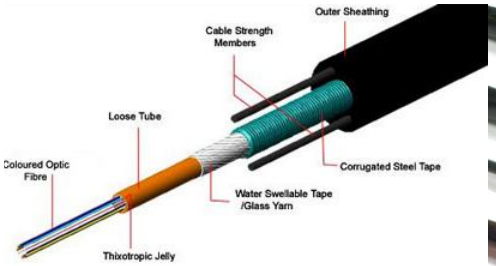


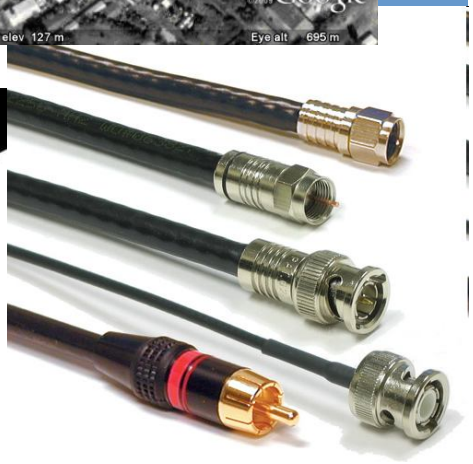
Példa 1: fizikai réteg

- Wifi hálózat lefedettségének vizsgálata
- hálózati kábelek
- hálózati csatlakozók





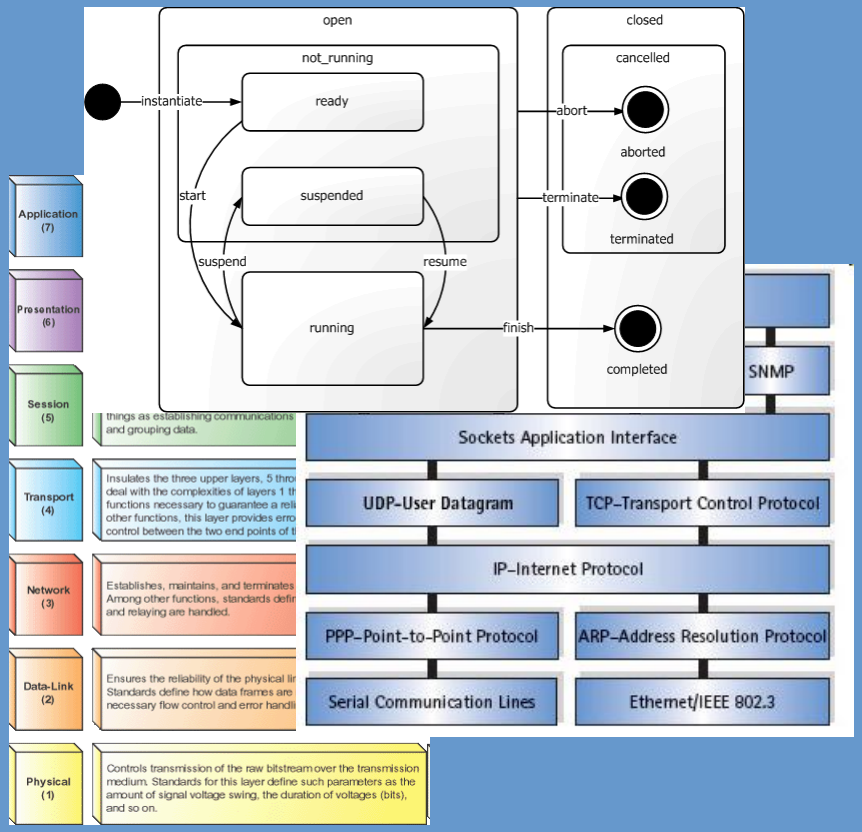




Médiamenedzsment réteg

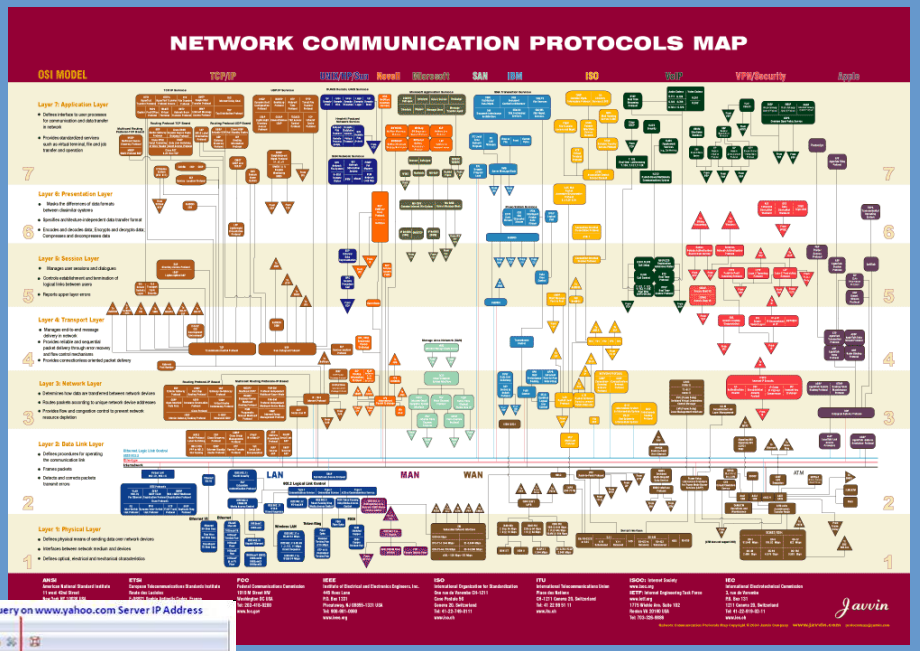
- Hálózat
  - a hálózati eszköz által küldött/fogadott adatok és üzenetek
    - ISO/OSI protokoll információk
    - küldött/fogadott adatok

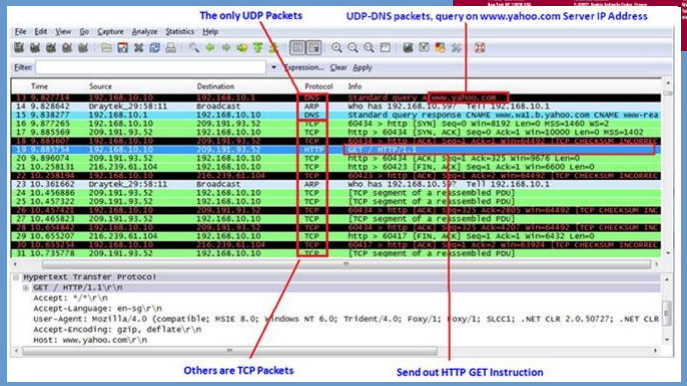
(*Hol vannak/lehetnek adatok?*)



Példa 2: médiamenedzsment réteg

- keret, csomag, adat
- TCP/IP protokollstruktúra
- os fingerprinting ≈ tool fingerprinting

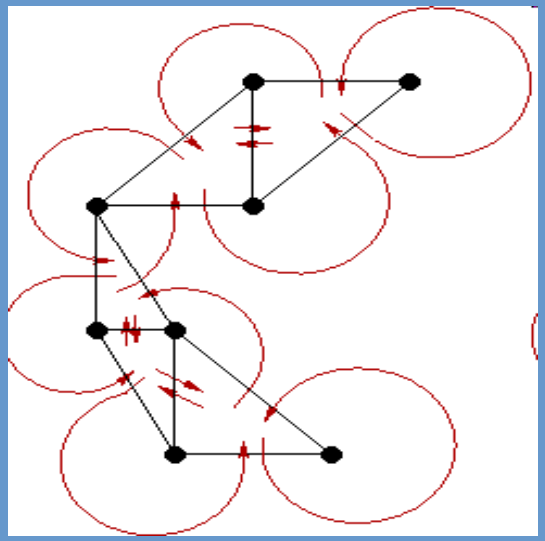




Megjelenítési réteg

- A tárolt adatok (adatfájlok) belső szerkezete, kódolása és sajátosságai

(*Milyen adategységek – pl. fájlok – vannak az „adatfolyamban”, ezek hogyan értelmezhetők?*)

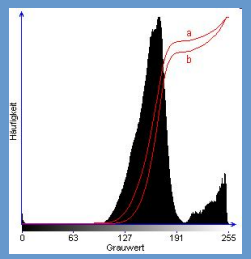


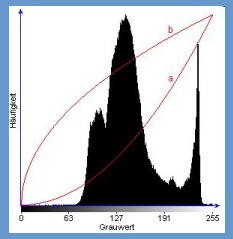
Példa 3: megjelenítési réteg

Média metaadatok

- EXIF (jpeg)
- IDAT (png)
- id3 (mp3)
- VorbisComments (ogg)
- geotagging
- …

Eredeti, módosított, hamis?





Példa 4: megjelenítési réteg

- Adategységek
  - egyedi fájlok
    - foglalt/hasznos adat (fájl)
    - törölt adat
    - fájl metaadatok (pl. MAC)
  - adat maradvány (slack space)
- Protokoll gráf információk
- Data carving

Alkalmazási réteg

- Adatok szakma-specifikus értelmezése
- Egyedi/speciális programok

(*Mi az adategység információtartalma?*)

Példa 5: alkalmazási réteg

- Alkalmazás, program egyedi sajátosságok
  - logika
  - beállítás (*.config, *.ini)
  - napló
- Alkalmazás visszafejtés (reverse engineering)
- Adatok értelmezése és információtartalma
- Nem IT szakértői feladatok
  - azonosítás (Lagzi Lajcsi?)
  - minősítés (csalás?)
  - szakma-specifikus értelmezés (grafológia, pszichológia, orvostudomány stb.)

Nyitott kérdések

- Kutatás: új eszközök és technológiák
- Számítógépes hálózat vizsgálati módszertani levél
  - vizsgálati folyamat
  - vizsgálati eszközök/eljárások
- Oktatás (főleg: szakértők, nyomozó hatóság képviselői)
- Anyagi források (pályázatok)