Bevezetés a Szteganalízisbe

Unicsovics György

e-mail: gy.unicsovics@nbh.hu

HTE előadás, Budapest **2007. november 19.**

Áttekintés:

- A szteganográfia rövid áttekintése;
- Szteganalízis:
  - ✓ Bevezetés a szteganalízisbe;
  - ✓ A fogvatartottak problémája;
- A szteganalízis lépései:
  - ✓ Érzékelés;
  - ✓ Kinyerés;
  - ✓ Megsemmisítés;
- A szteganográfia támadása:
  - ✓ Támadások osztályozása;
- A szteganalízis eszközei:
  - ✓ Alkalmazások;
  - ✓ Szoftverek értékelése;
- Összegzés.

A szteganográfia története

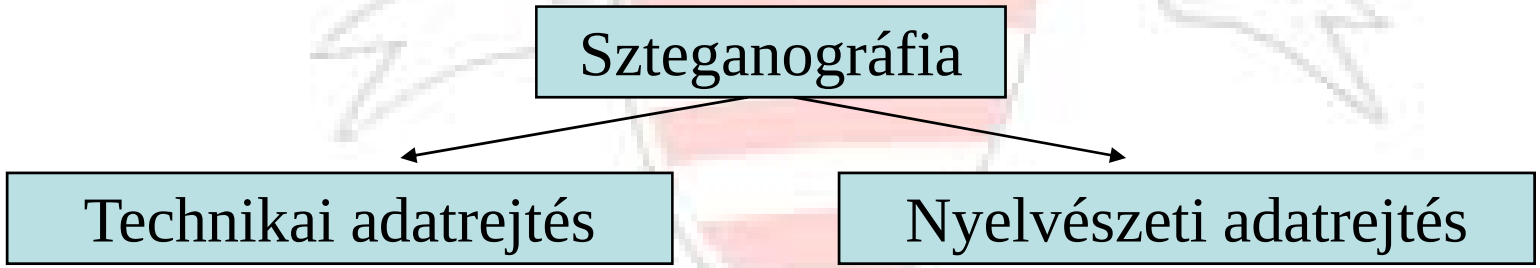
Steganography ≠ Stenography

Már az ókoriak is.....

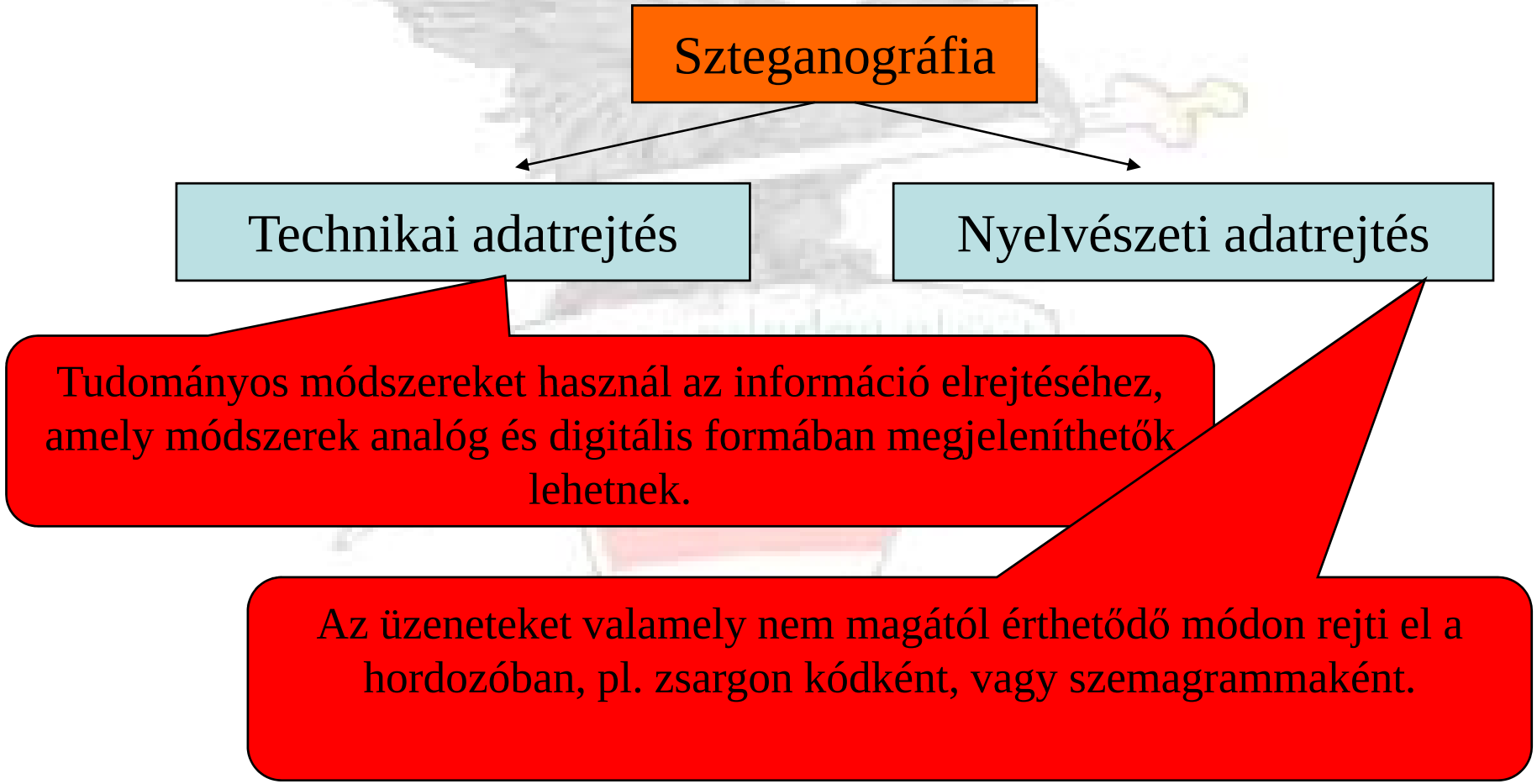
Szteganográfia jelentése és célja:

- Szteganográfia a rejtett, vagy fedett írás művészete. Célja a kommunikáció tényének elrejtése a harmadik fél elől.

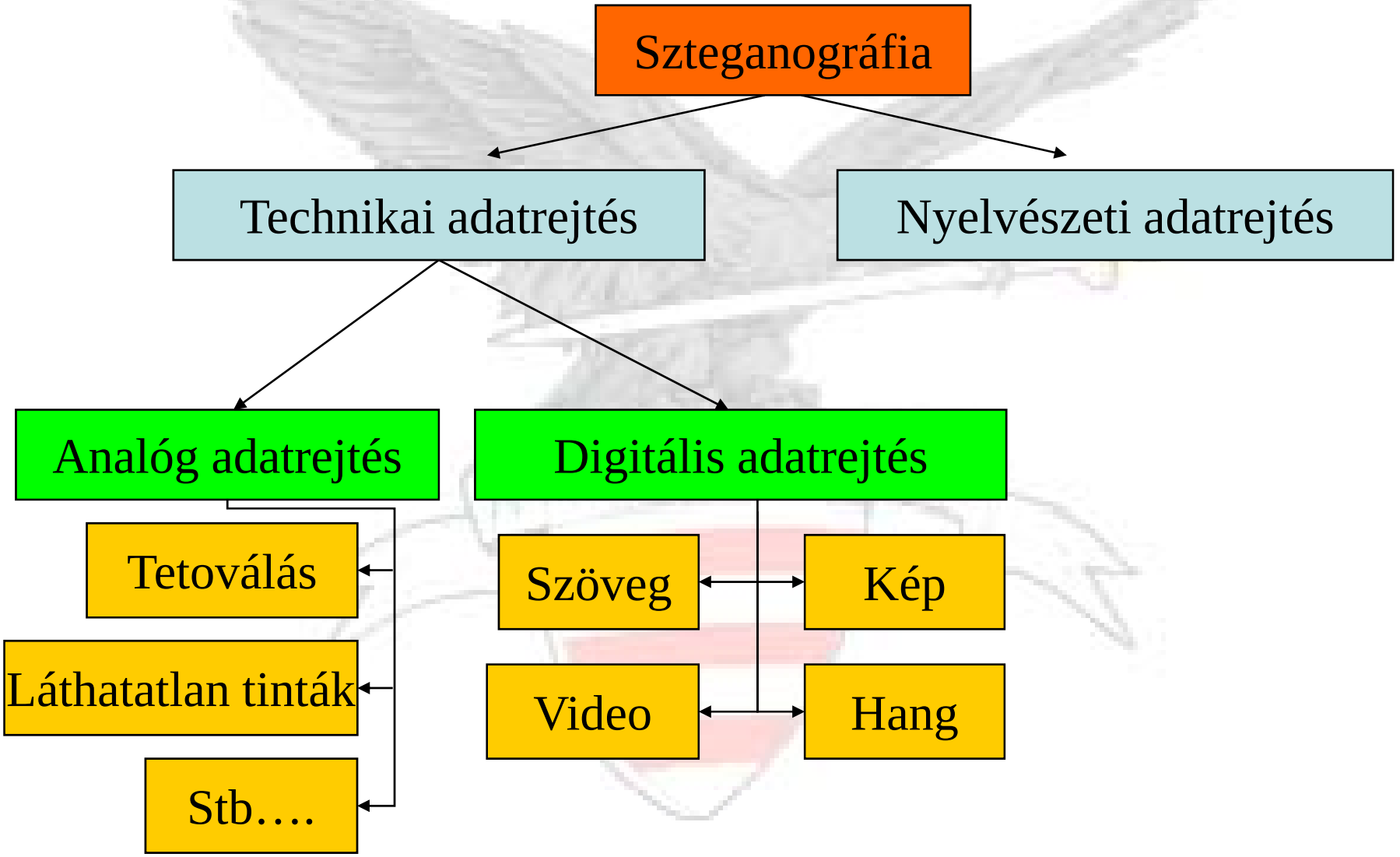
Szteganográfia fő csoportjai:

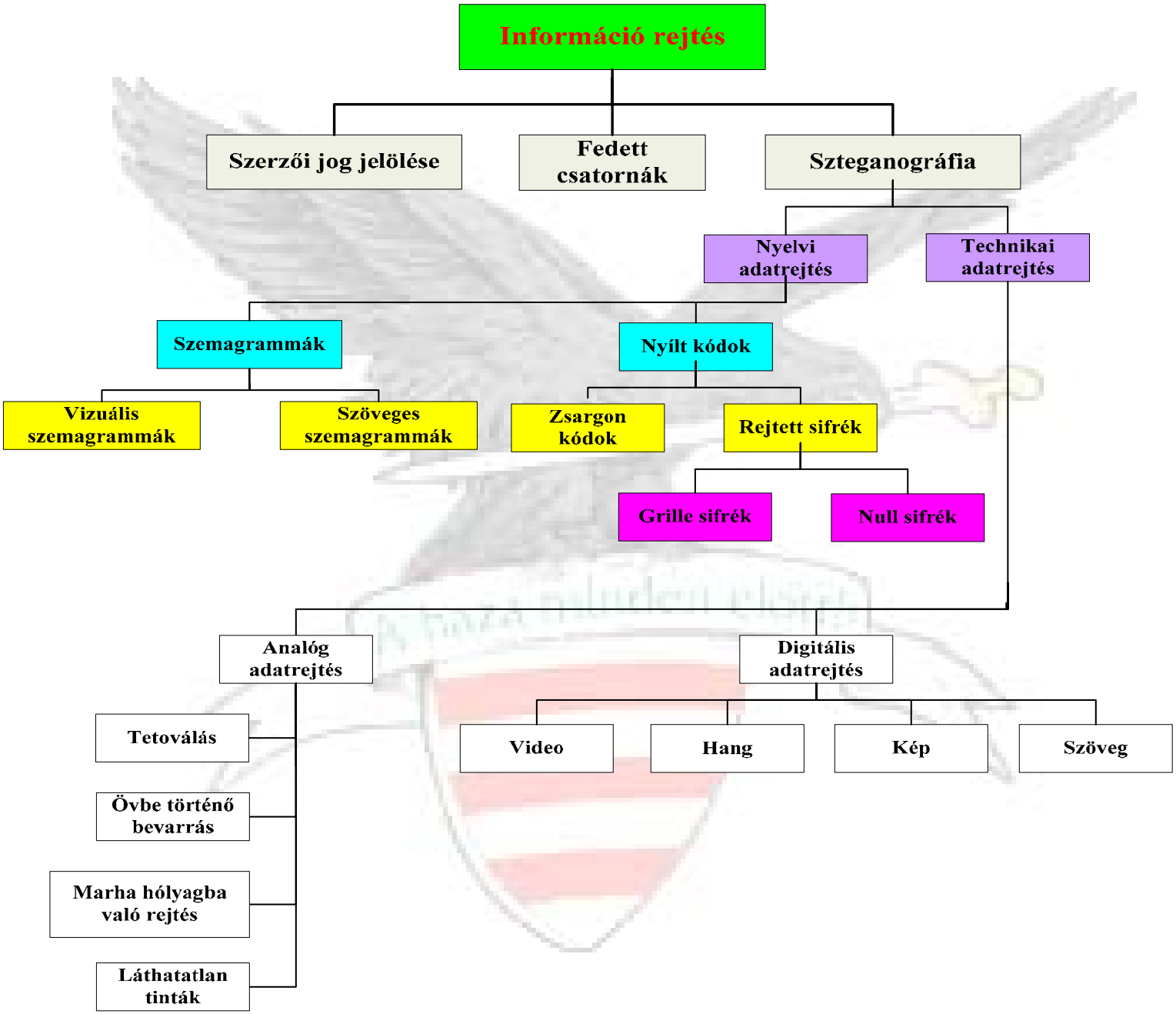


Szteganográfia felosztása



Szteganográfia felosztása folyt.




Információ rejtés
Szerzői jog jelölése
Fedett csatornák
Szteganográfia
Nyelvi adatrejtés
Technikai adatrejtés
Szemagrammák
Nyílt kódok
Vizuális szemagrammák
Szöveges szemagrammák
Zsargon kódok
Rejtett sifrék
Grille sifrék
Null sifrék
Analóg adatrejtés
Digitális adatrejtés
Tetoválás
Övbe történő bevarrás
Marha hólyagba való rejtés
Láthatatlan tinták
Video
Hang
Kép
Szöveg

Bevezetés a szteganalízisbe

Szteganalízis jelentése és célja:

- Szteganalízisnek nevezzük a rejtett információk észlelésének eljárását, melynek célja a rejtett kommunikáció felfedése.

- Nincs információ kinyerés!!!

- Nincs információ megfejtés!!!

- Védelmi szempontból az észlelés kevés!!!!

Bevezetés a szteganalízisbe folyt.

Hogyan tehetünk eleget a védelmi igényeknek?

- A szteganalízis eljárásban detektálni kell a hordozóban elrejtett üzenetet;
- A detektált üzenetet ki kell nyerni a hordozóból;
- A kinyert üzenetet meg kell fejteni.

Bevezetés a szteganalízisbe folyt.

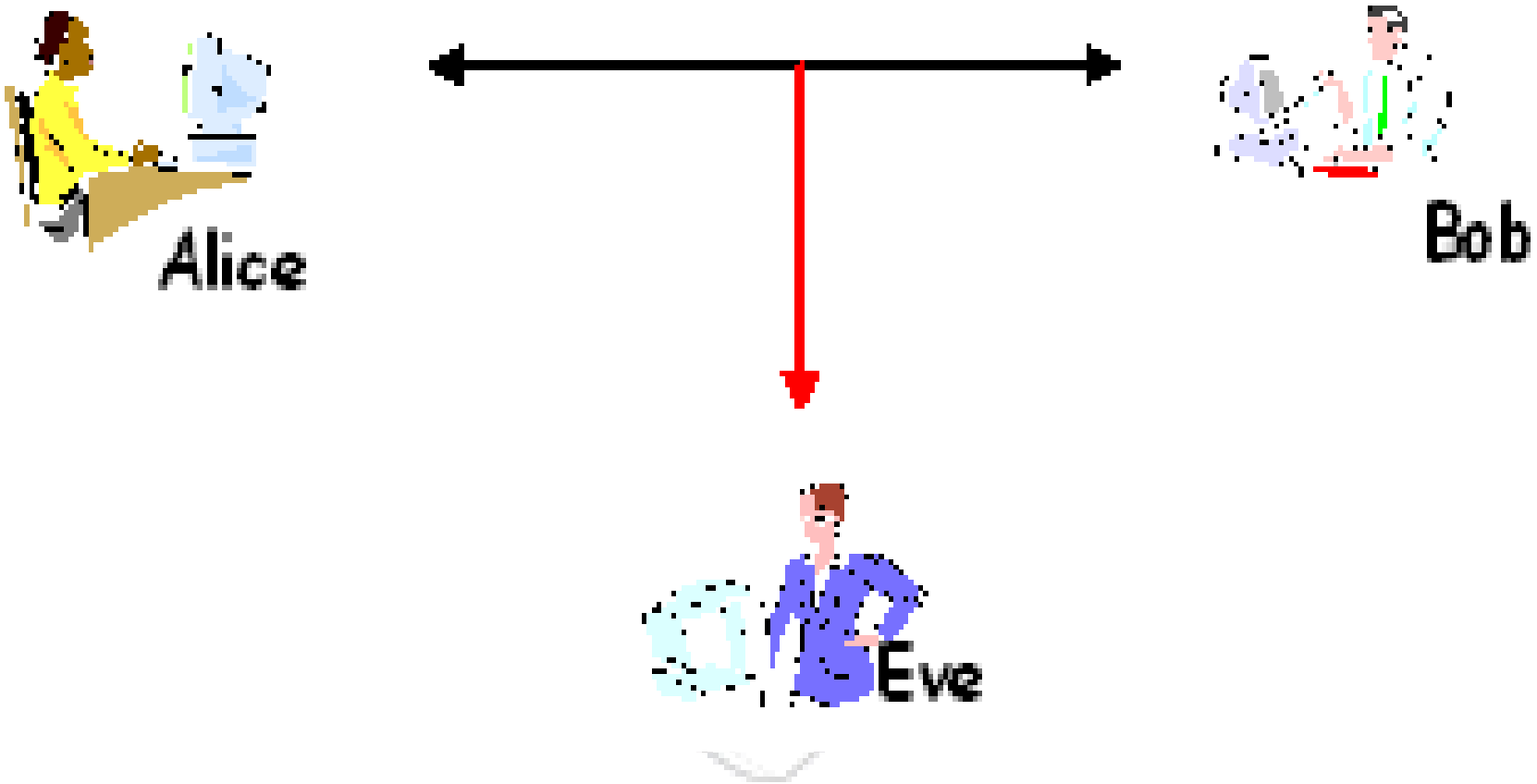
A szteganográfiai támadások célja…….

hogy a sztegomédiában felfedjük az eredeti hordozóhoz képesti változásokat, függetlenül attól, hogy ezek okoztak e szemmel érzékelhető változást az eredeti állományhoz képest.

A támadási módszerek megválasztása és a támadás kivitelezése elsődlegesen nem függvénye az alkalmazott szteganográfiai szoftvertnek.

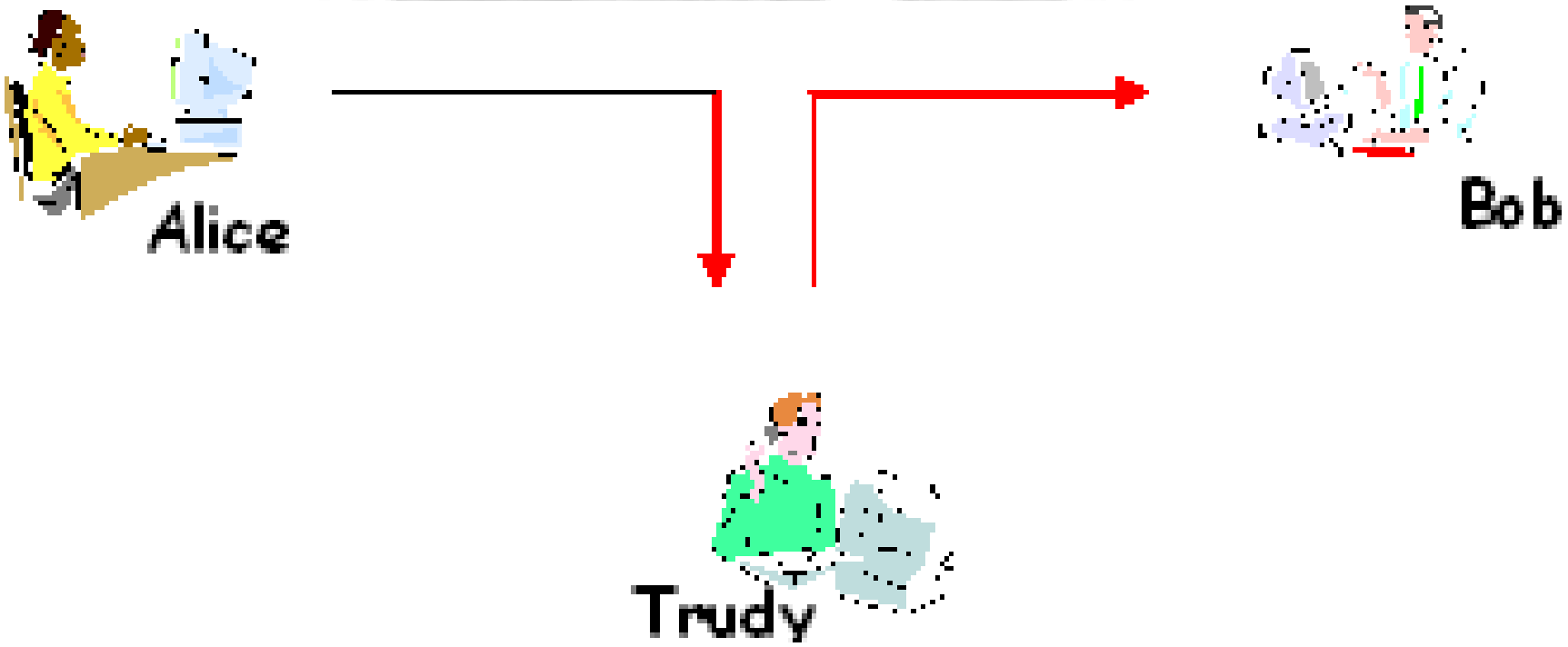
Fogvatartottak problémája.....

Passzív támadás:



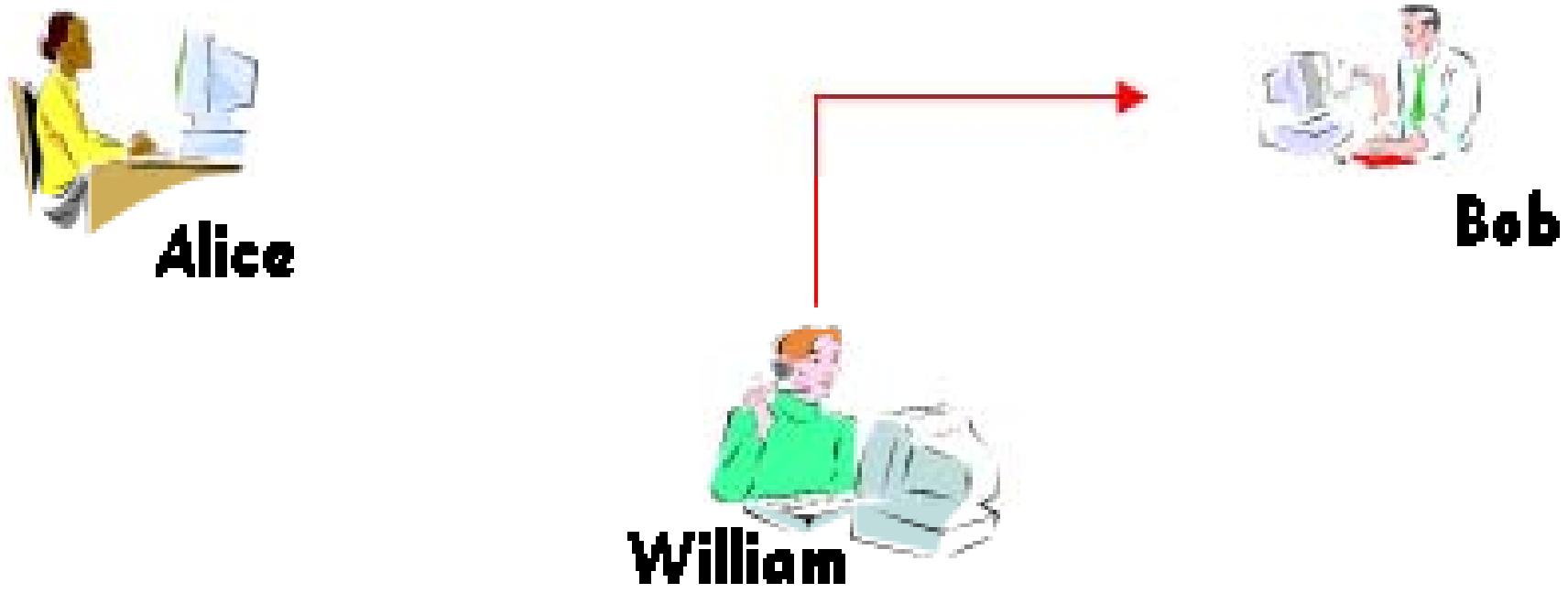
Fogvatartottak problémája.....foyt.

Aktív támadások:



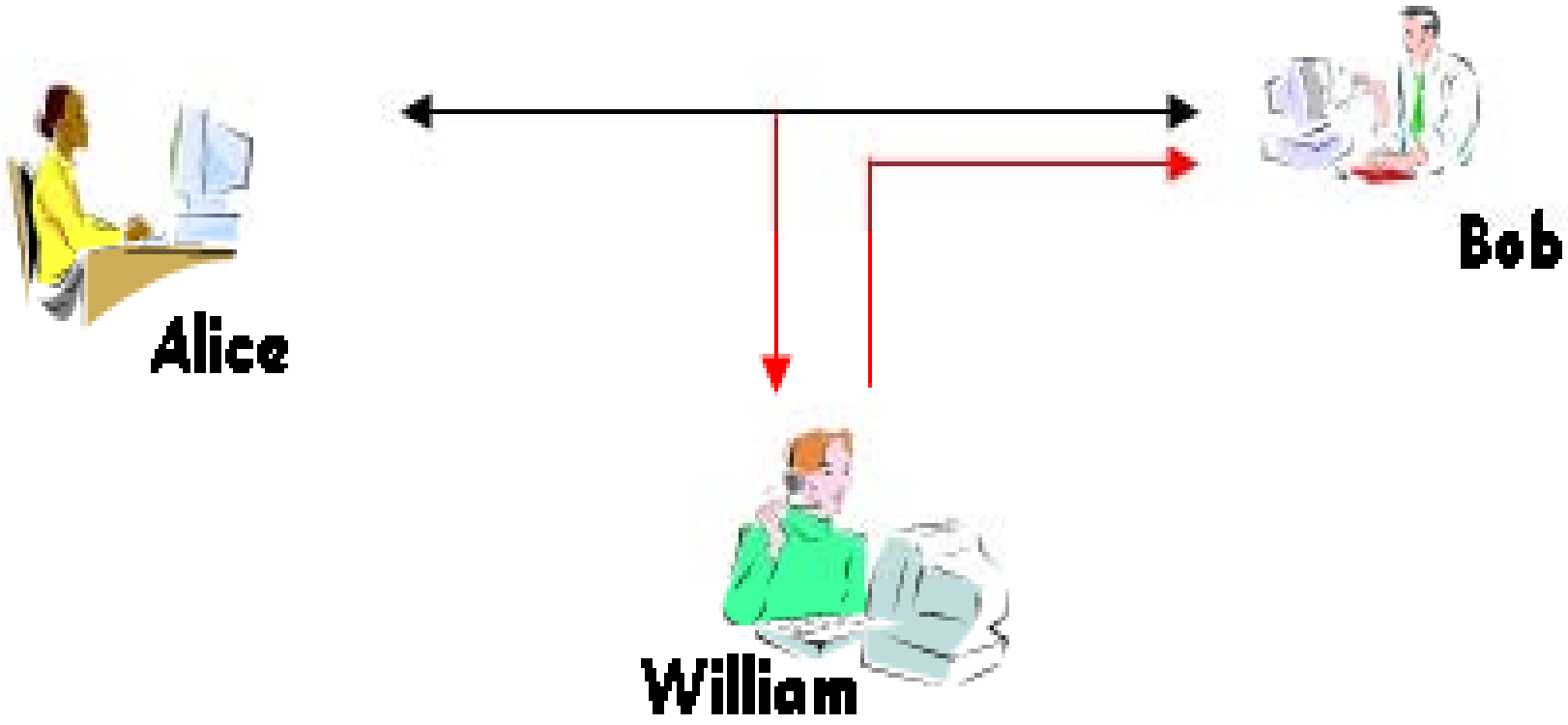
Általános szándékú aktív támadás

Fogvatartottak problémája.....foyt.



Üzenet hamisítási szándékú aktív támadás

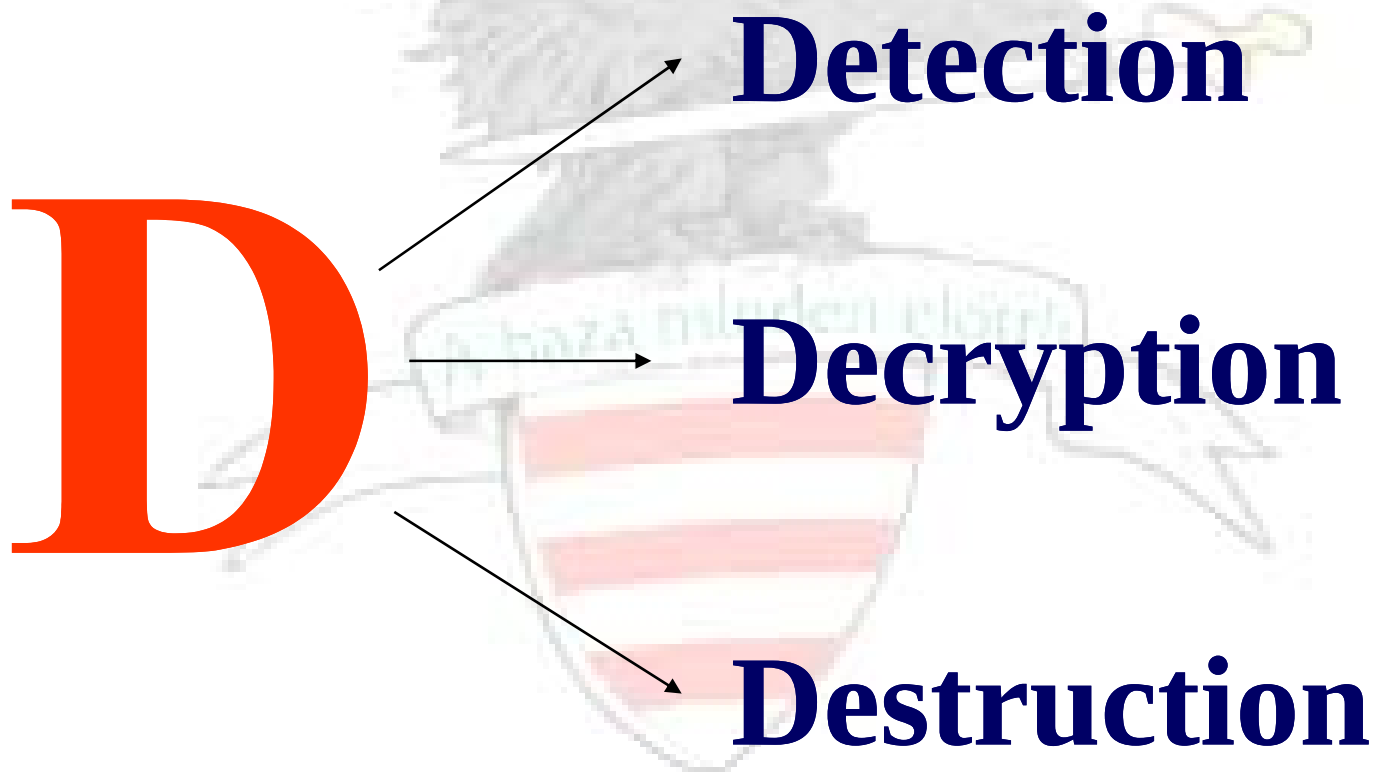
Fogvatartottak problémája.....foyt.



Aktív támadás üzenet ismételt, módosított küldésével

A szteganalízis lépései

A szteganalízist leírhatjuk mint a szteganográfiai eljárások megelőzésére irányuló tevékenységet.



A szteganográfia támadása

A következő támadási eljárásokat ismerjük:

- Csak a sztegoobjekt támadása (Stego-only attack);

- Ismert hordozó támadása *(Known cover attack);*

- Ismert üzenet támadása *(Known message attack);*

- Választott sztegoobjekt támadása *(Chosen stego attack);*

- Választott üzenet támadása *(Chosen message attack);*

- Ismert szteganográfiai támadás (*Known stego attack*);

Szteganográfia Detektálhatósága

- **Egyszerű szteganográfiai modell esetén a harmadik fél semmit nem tud az alkalmazott módszerről;**
- **Rejtjelzéssel kombinált szteganográfia esetén, a börtönőr ismeri a sztego algoritmust, azonban nem ismeri a titkos kulcsot, amelyet a kommunikáló felek használnak;**
- **Napjaink sztegoanalízise még erős fejlődésben van, az első cikkek ez irányban a késői ’90-es években láttak napvilágot;**
- **Uniformizálás szükségessége.**

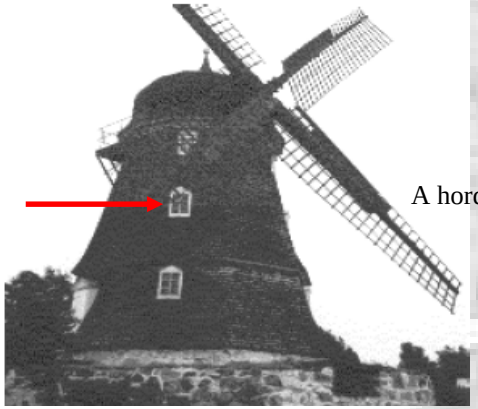
Szteganográfia Detektálhatósága folyt.

A detektálás osztályozása történhet:

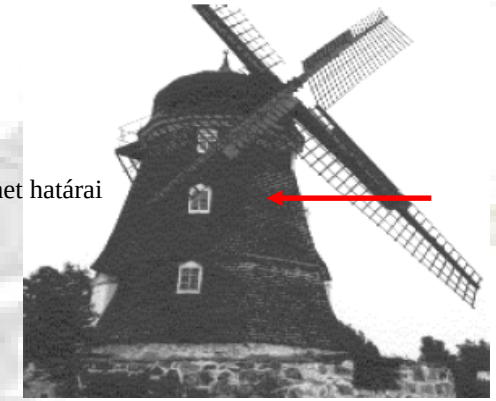
- **Fájl aláírások;**
- **Fájl anomáliák;**
- **Vizuális támadások;**
- **Statisztikai támadások;**

Szteganográfia Detektálhatósága folyt.

Vizuális támadások:

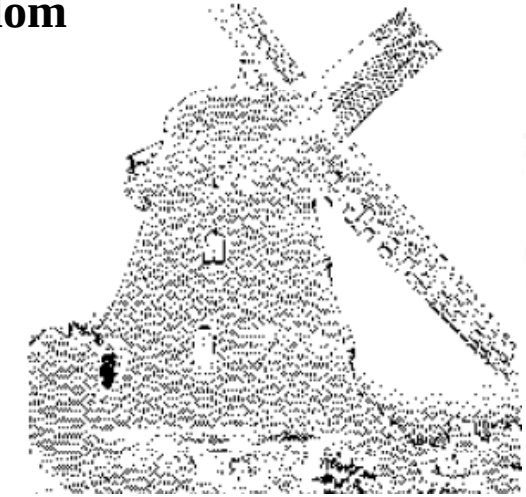


A hordozó és a rejtett üzenet határai megfigyelhetők



Eredeti hordozó **Rejtett üzenet tartalom**

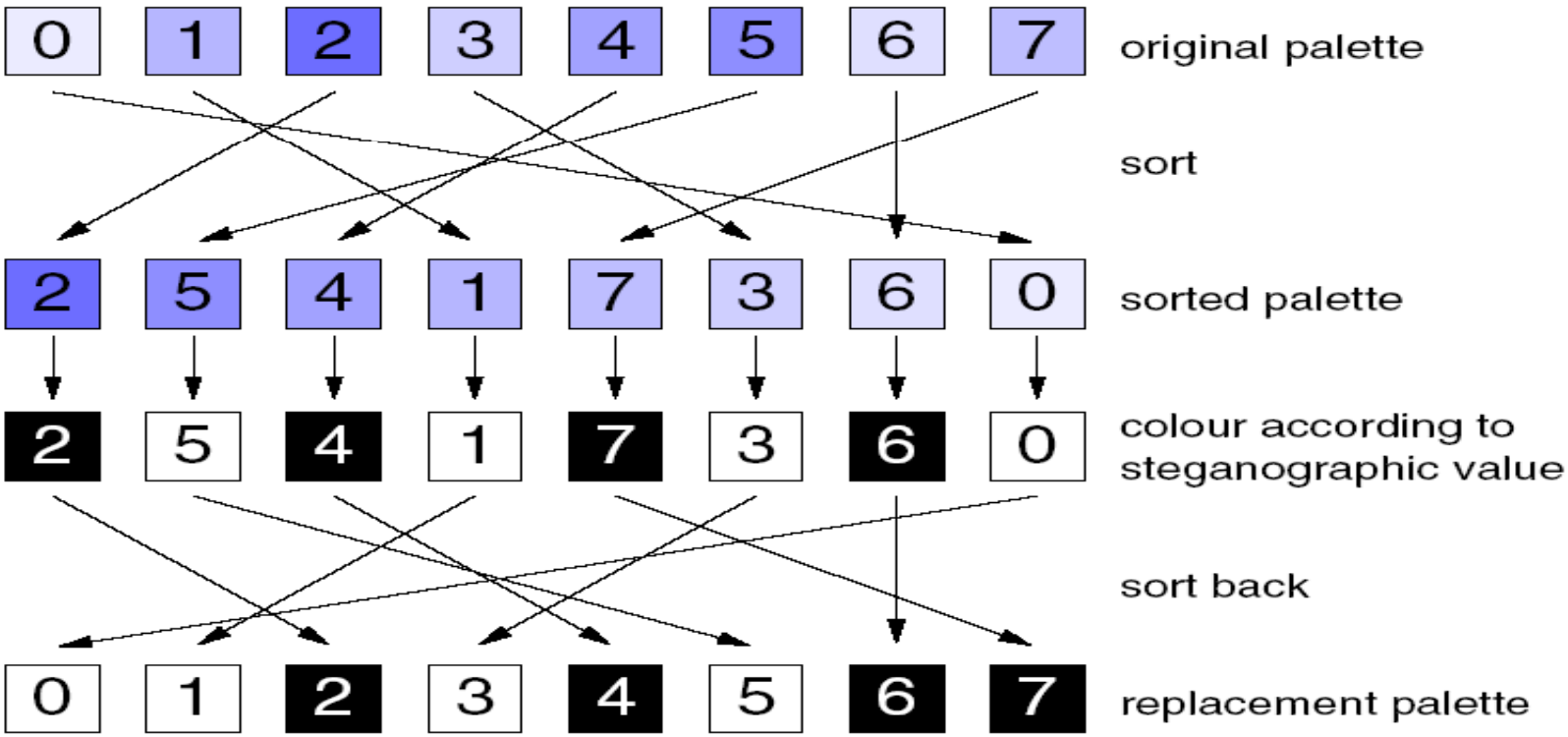
LSB=0 ha fekete



LSB=1 ha fehér

Szteganográfia Detektálhatósága folyt.

Vizuális támadások:



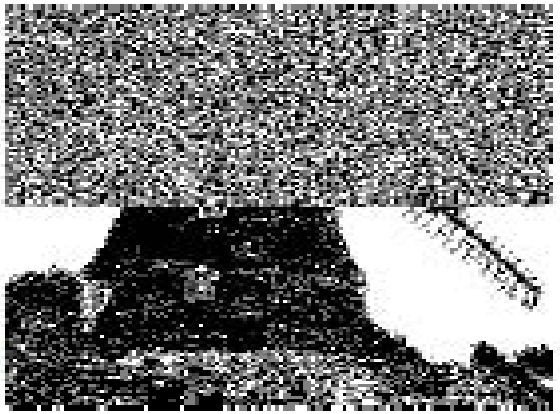
Szteganográfia Detektálhatósága folyt.

Vizuális támadások:

Eredeti hordozó

Rejtett üzenet

Szűrt A

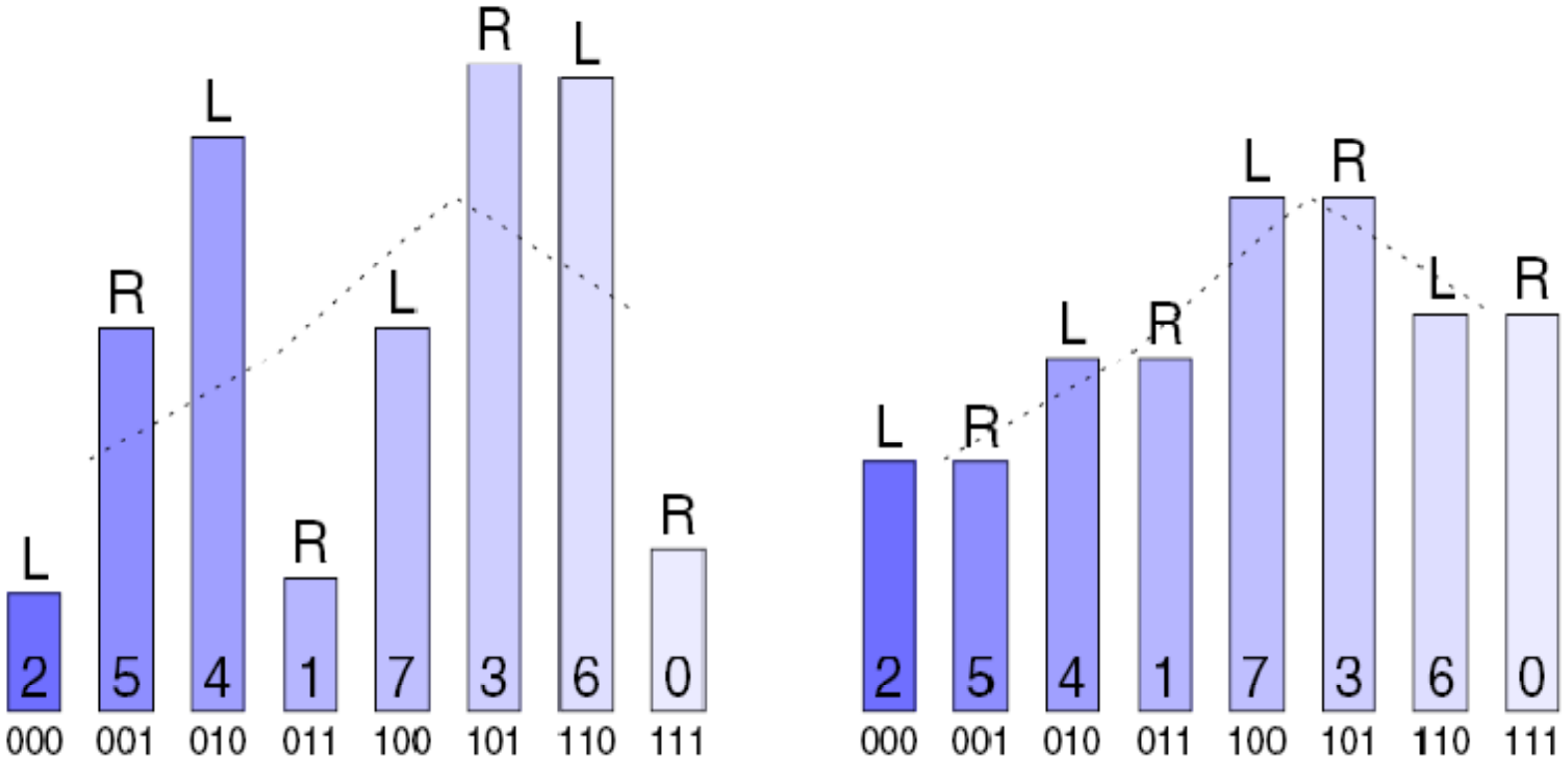


Szűrt B

Szteganográfia Detektálhatósága folyt.

Statisztikai támadások:

Chi-square Attack



A szteganalízis eszközei

A szteganográfia detektálására hivatott szoftvereket szteganalitikai eszközöknek hívjuk.

Néhány szabadon felhasználható, néhányuk fiztetős és meglehetősen drága.

A rejtett információ detektálása után a beágyazott tartalmat ki kell nyerni a hordozóból.

Néhány szteganalitikai szoftver:

Szoftver neve	Detektált média	Licence	Fejlesztő/gyártó
StegSpy	JPEG	Szabadon felhasználható	Michael T. Raggo
Stegdetect	JPEG	Nyílt forrású	Niels Provos
StegBreak	JPEG	Nyílt forrású	Niels Provos
StegSuite		Licence díjas	Wetstone Technologies
StegAnalyzer	JPEG	Licence díjas	Wetstone Technologies

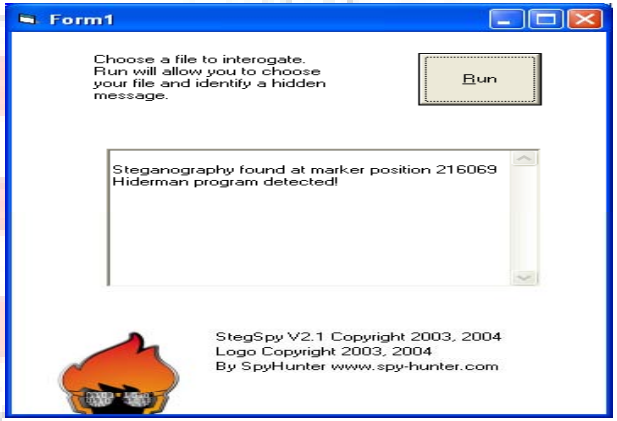
A szteganalízis eszközei folyt.

Stegspy:

25/a Eredeti hordozó (1.1 MB)

25/b StegSpy analízis eredménye

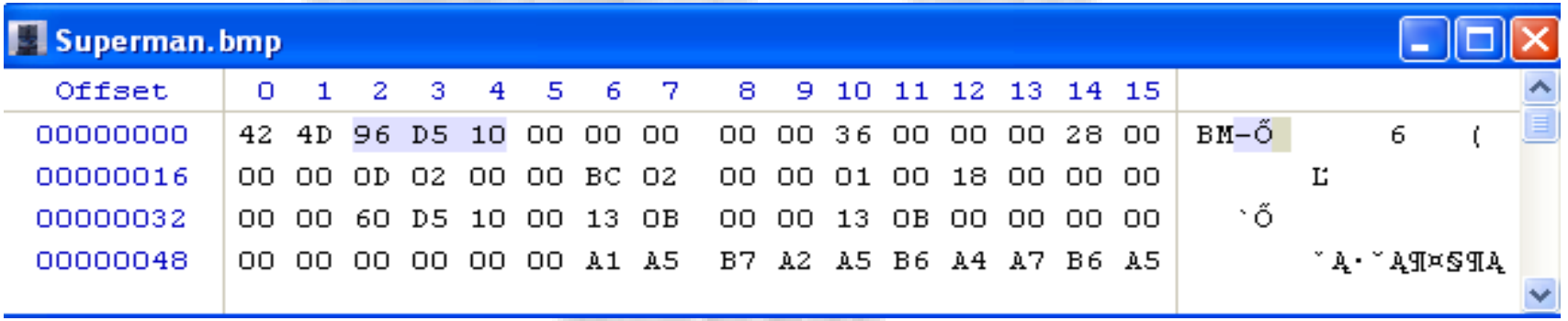
Beágyazott állományt tartalmazó hordozó (108,5 KB)



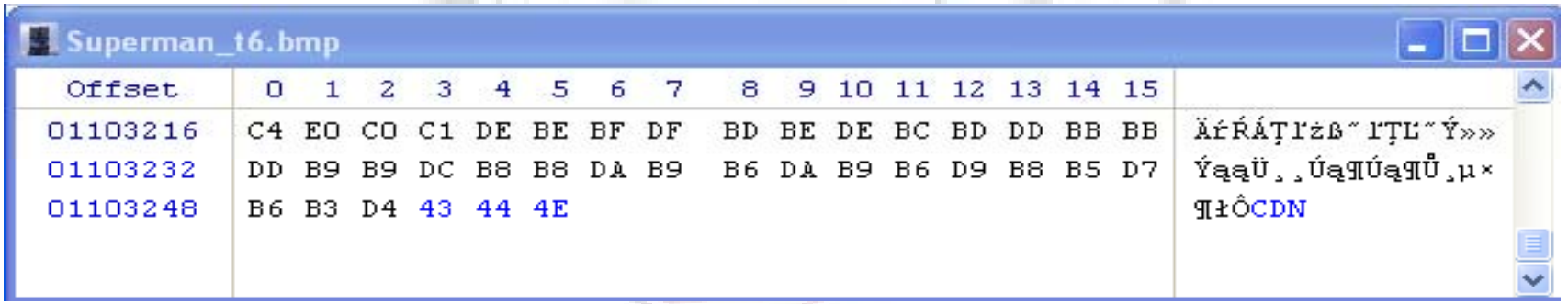
Beágyazott állomány a hordozóban, a 216069-os poziciótól kezdődően

A szteganalízis eszközei folyt.

Stegspy:



A BMP fájl fejlécének kezdete



A BMP fájl fejlécének vége

A szteganalízis eszközei folyt.

Stegdetect:

JPEG fájl detektálása a Stegdetect programmal

A szteganalízis eszközei folyt.

Stegbreak:

- **Niels Provos által kifejlesztett alkalmazás;**

- **DOS alatt futó alkalmazás, ami teljes kipróbálású szótár-támadások elvégzését teszi lehetővé JPEG formátumú képek ellen.**

- **A támadás során a beágyazásnál használt jelszó megfejtése után az elrejtett információt nyeri ki a hordozóból.**

- **A Stegbreak sikere természetesen szorosan összefügg a jelszó és a könyvtár minőségétől. A szavak könyvtárban történő változtatásának szabálya szintén szorosan összefügg a sikerrel.**

A szteganalízis eszközei folyt.

StegoSuite:

A WetStone által kifejlesztett szoftver széles körben elterjedt az igazságügyi szakértői körökben, mivel lehetővé teszi a szteganográfiai módszerek teljes tárházának felfedését.

StegoSuite moduljai:

StegoAnalyst;

StegoBreak;

StegoWatch;

A szteganalízis eszközei folyt.

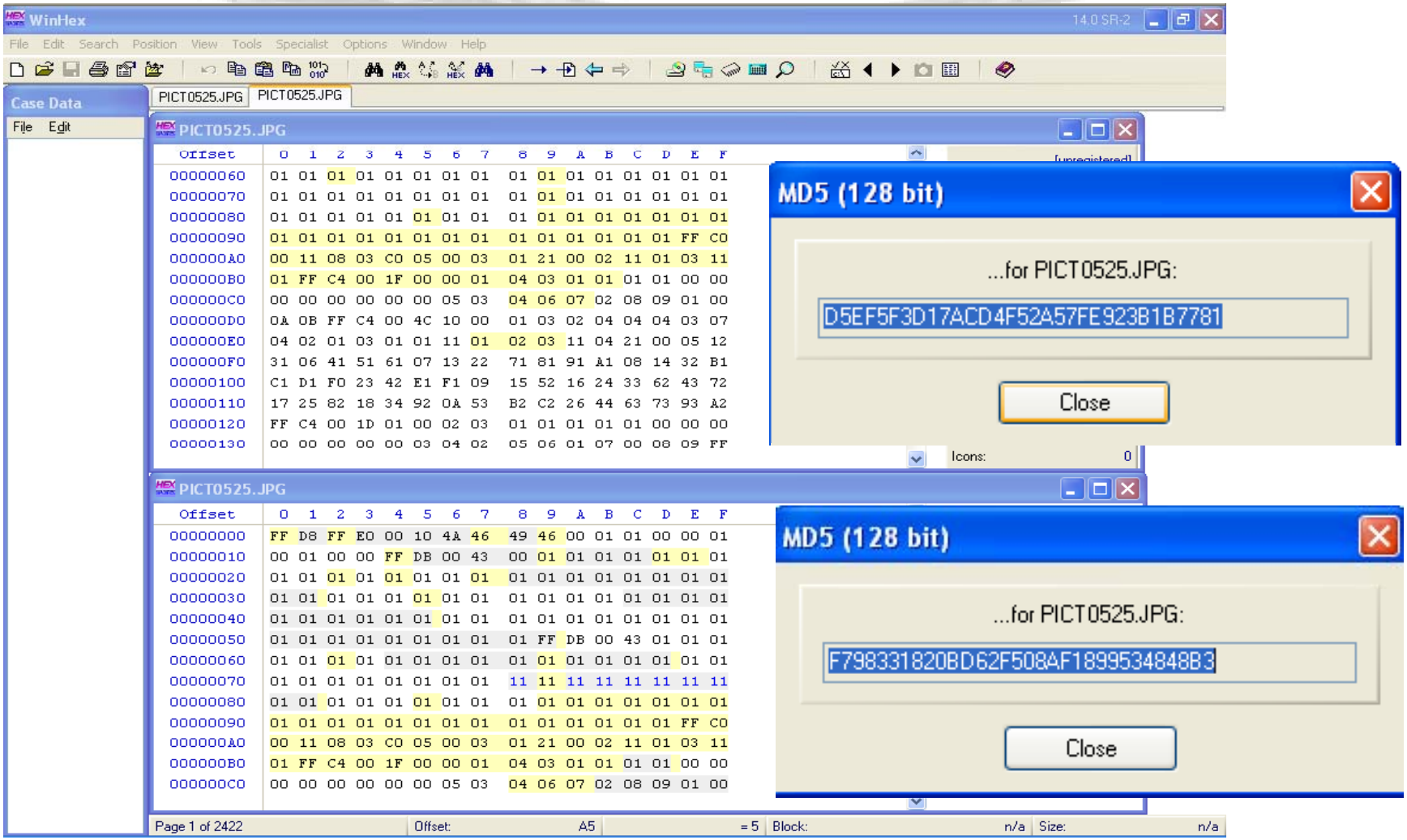
StegAnalyzer:

Jelenleg a Backbone Security két verzióban kínálja a StegAnalyzer-t:

- **A StegAnalyzer AS fájlrendszerek felderítésére szolgál, azokat képes átkutatni, ismert szteganográfiai szoftverek nyomait keresve.**
- **A StegAnalyser SS képes az ismert sztegoobjektum fájlaláírások detektálására, amellett, hogy az AS modifikáció valamennyi képességével bír.**

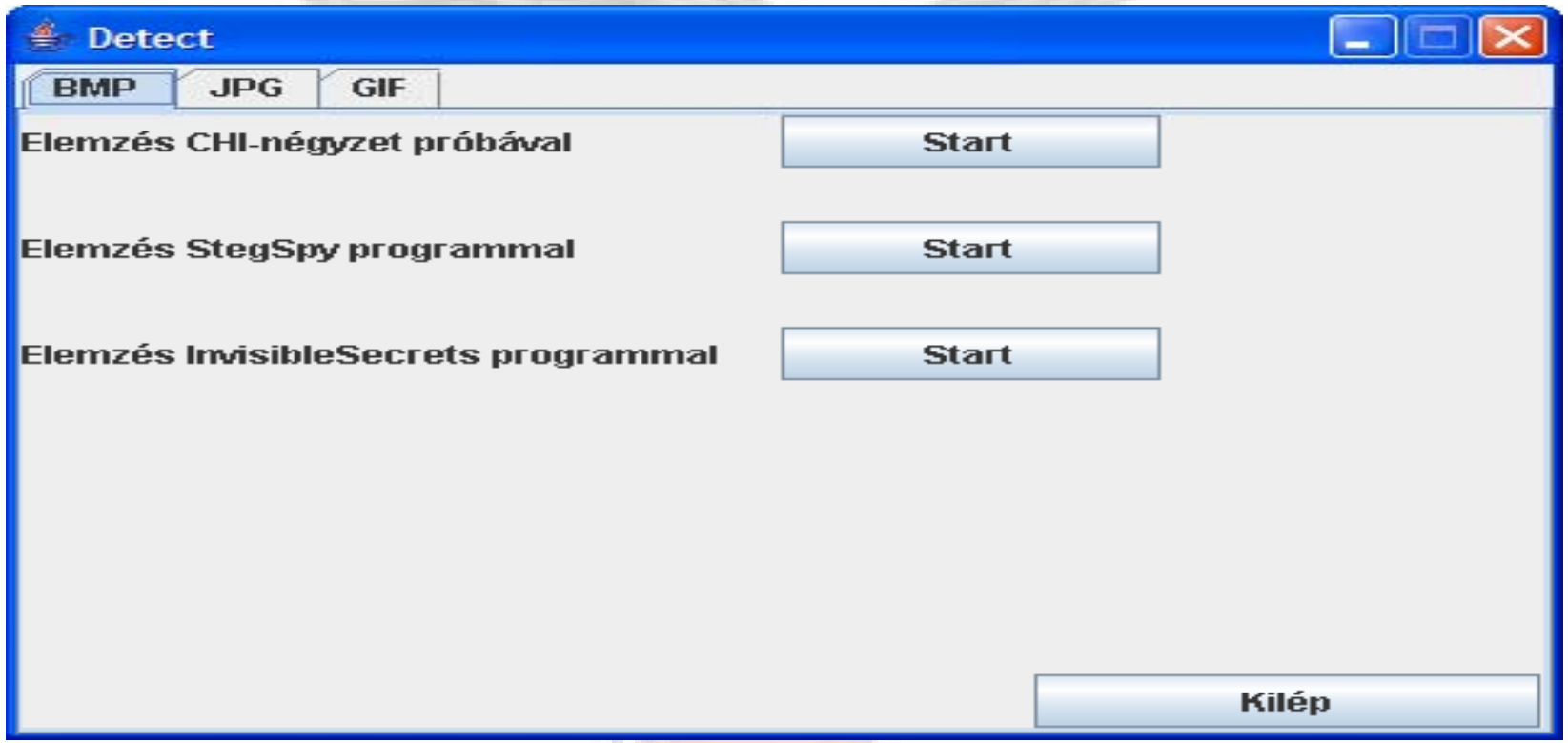
A szteganalízis eszközei folyt.

WinHex:



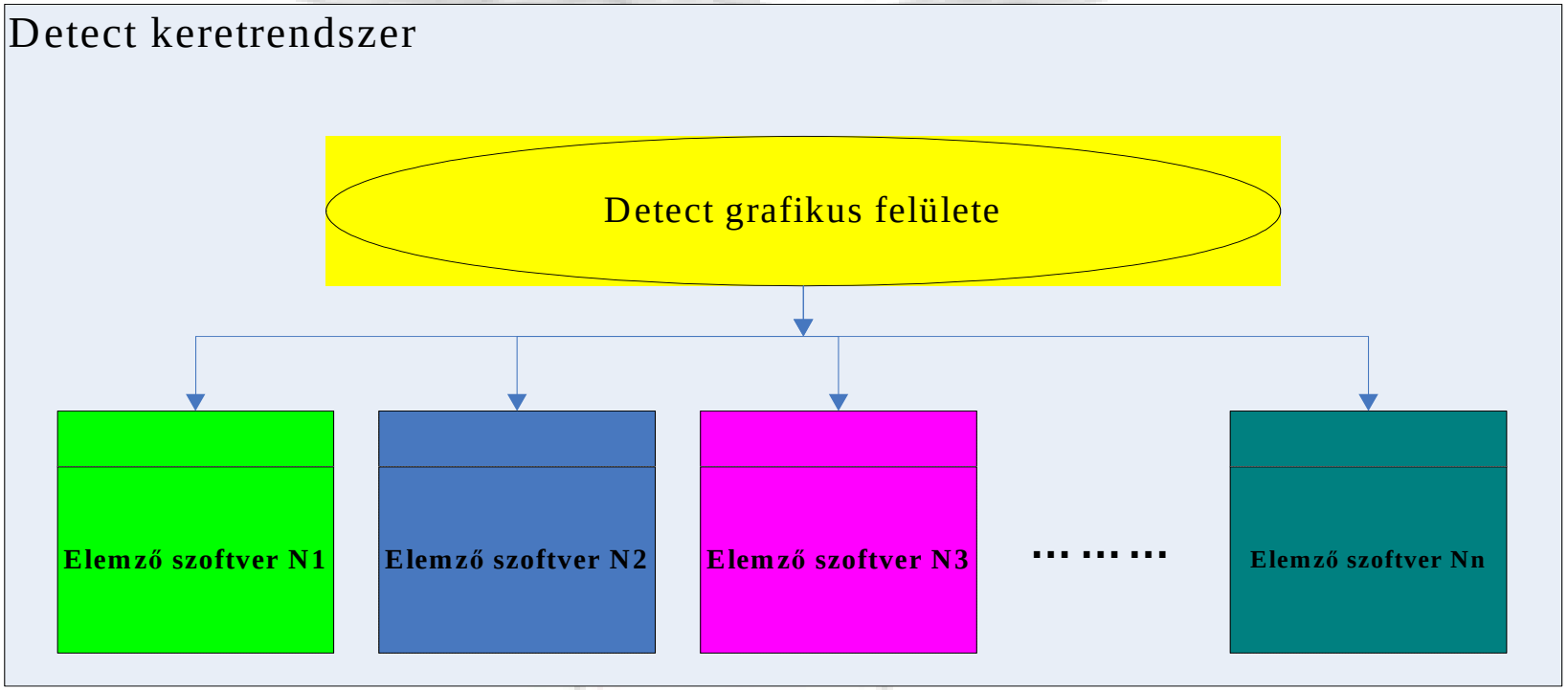
A szteganalízis eszközei folyt.

Detect:



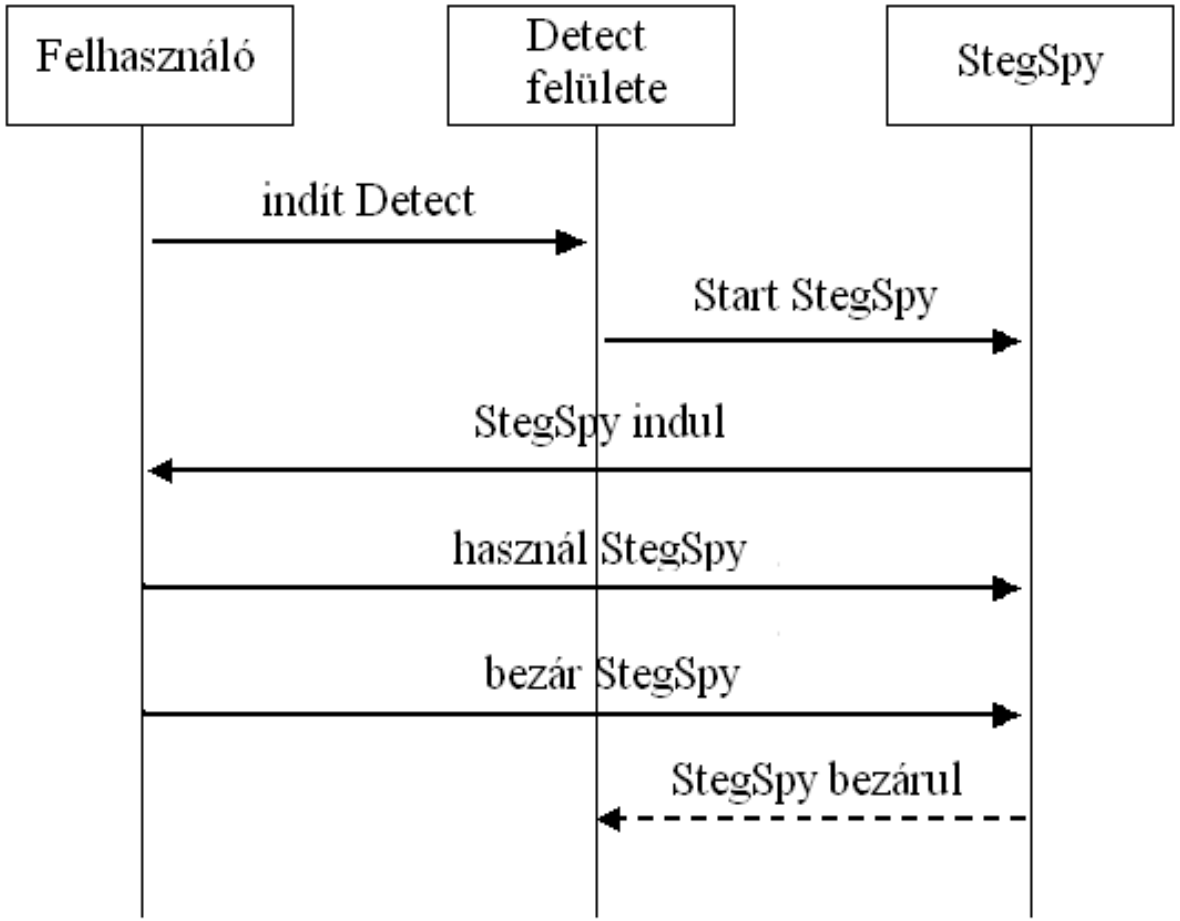
A szteganalízis eszközei folyt.

Detect:



A szteganalízis eszközei folyt.

Detect:



A szteganalízis eszközei folyt.

Detect:

Továbbfejlesztési irányok:

- a keretrendszerben a jövőben még több analizáló szoftver jelenhet meg, mely nem csak a jelenlegi hordozómédiákra biztosít több elemzési lehetőséget, hanem újabb hordozómédiát is képes vizsgálni;

- a Detect bemenetére érkező sztegoobjektum paraméterei alapján kerül automatikusan kiértékelésre, majd az eredménynek megfelelően automatikusan elindul a Detect megfelelő moduljának futása;

A szteganalízis eszközei folyt.

Detect:

Továbbfejlesztési irányok:

-a keretrendszerből indítható analizáló szoftverek bővülésével párhuzamosan merül fel az igény, hogy a Detect több szálon tudjon futni oly módon, hogy egyszerre többféle médián, több elemzés legyen végrehajtható.

A Szteganográfia észlelésének problémái

- **Relatíve új és gyorsan fejlődő tudomány;**
- **Magas a „false positive” szám;**
- **hatalmas mennyiségű képi média, valamint majdnem mindegyikre létező szteganográfiai alkalmazás ;**
- **nagy monotonitású képek és rajzok esetében szintén magas „false positive”;**
- **kifejezetten problémás a kis terjedelmű üzenetek detektálása;**
- **titkosítás alkalmazása a szteganográfiai szoftverekben.**

Igazságügy vs. Szteganográfia

- **A szteganográfia természetes törekvése, hogy rejtve maradjon. Nincs kellő publicitása az igazságügyi oldalról elért eredményeknek, nincs statisztika.**

- **A szteganográfia hatásainak mellőzése a statisztikai hiányosságok miatt rossz alternatíva.**

- **Természetes azt feltételezni, hogy a szteganográfiát használják, vagy használni fogják, mivel jellegzetessége a rejtés, ami vonzó a bűnözők számára.**

- **Ezért, ha a bűnözők még nem is használják a szteganográfiát, a jövőben a cyberspace bűnözők által alkalmazott eszközökben biztosan felbukkannak majd a szteganográfia különböző adaptációi.**

A szteganográfia legyőzése

- **A szteganográfiai alkalmazások legyőzésének folyamata hasonlít a kriptoanalízishez. Az előforduló gyenge pontok feltárására koncentrál.**

- **Néhány megközelítés a statisztikai változásokat (fájlanomáliák, furcsa paletták, ismert fájlaláírások stb.) vizsgálja, míg mások a vizuális felderítést helyezik előtérbe.**

- **Mindezek ellenére az igazságügyi szakértőknek más eszközök is rendelkezésükre állnak.**

A szteganográfia legyőzése folyt.

- digitális bűntény helyszínének vizsgálata;
- sztegelemzés;
- szteganográfiai szoftver detektálása;
- szteganográfiai szoftver nyomai;
- hordozó/sztegofájl párok lokalizálása;
- kulcsszó-keresés és aktivitás monitorozása;
- gyanúsított számítástechnikai ismeretei;
- valószínűtlen fájlok keresése;
- szteganográfiai kulcsok lokalizálása;
- rejtett tároló helyek;

Szteganográfiai alkalmazások

S-Tools

- GIF, BMP, WAV

JP Hide&seek

- JPEG

MP3Stego

- MP3

Steghide

- BMP, JPEG, WAV, AU

Szteganalitikai alkalmazások

StegSpy

- JPEG

StegDetect

- JPEG

Stegbreak

- JPEG

Detect

- BMP, JPEG, GIF, WAV, AU

Összegezve

- A szteganográfia nem más mint az információ elrejtésének módja egy kiválasztott hordozóba.
- A szteganalízis a rejtett információk felfedésére irányuló komplex tevékenységek összessége.
- Az interneten szabadon elérthető programok garmadája.
- Sokkal kevesebb publikált analitikai program, többségük borsos árakon.
- Az adatrejtés detektálása meglehetősen bonyolult, de nem lehetetlen feladat.
- Kombinált eljárások végrehajtása.
- Sok anekdóta kering a szteganográfia különösen terroristák általi használatáról.
- Nincs statisztikai kimutatás az analitikai szoftverek sikerességéről.
- Eddig senki nem talált erre nézve perdöntő bizonyítékot.

1997. Luisburg.....Árja Testvériség.

Hasznos linkek:

- http://www.stegoarchive.com/
- http://www.crazyboy.com/
- http://www.spammimic.com/
- http://www.wetstonetech.com/
- http://www.outguess.org/
- http://www.spie.org
- http://steganography.tripod.com/stego/software.html
- http://rr.sans.org/covertchannels/steganography3.php
- http://rr.sans.org/covertchannels/steganography3.php
- http://www.wired.com/news/politics/0,1283,41658,00.html
- http://www.darkside.com.au/snow
- http://www.heise.de/tp/english/inhalt/te/9751/1.html

Köszönöm, hogy meghallgattak!