



Bevezetés a Szteganalízisbe

Unicsovics György

e-mail: gy.unicsovics@nbh.hu

Hétpecsét előadás, Budapest

2008. január 16.

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

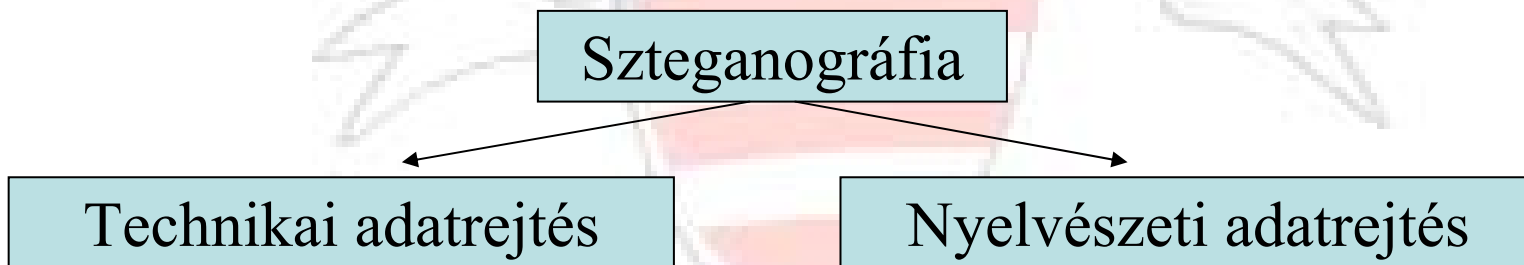
Steganography \neq Stenography

Már az ókoriak is.....

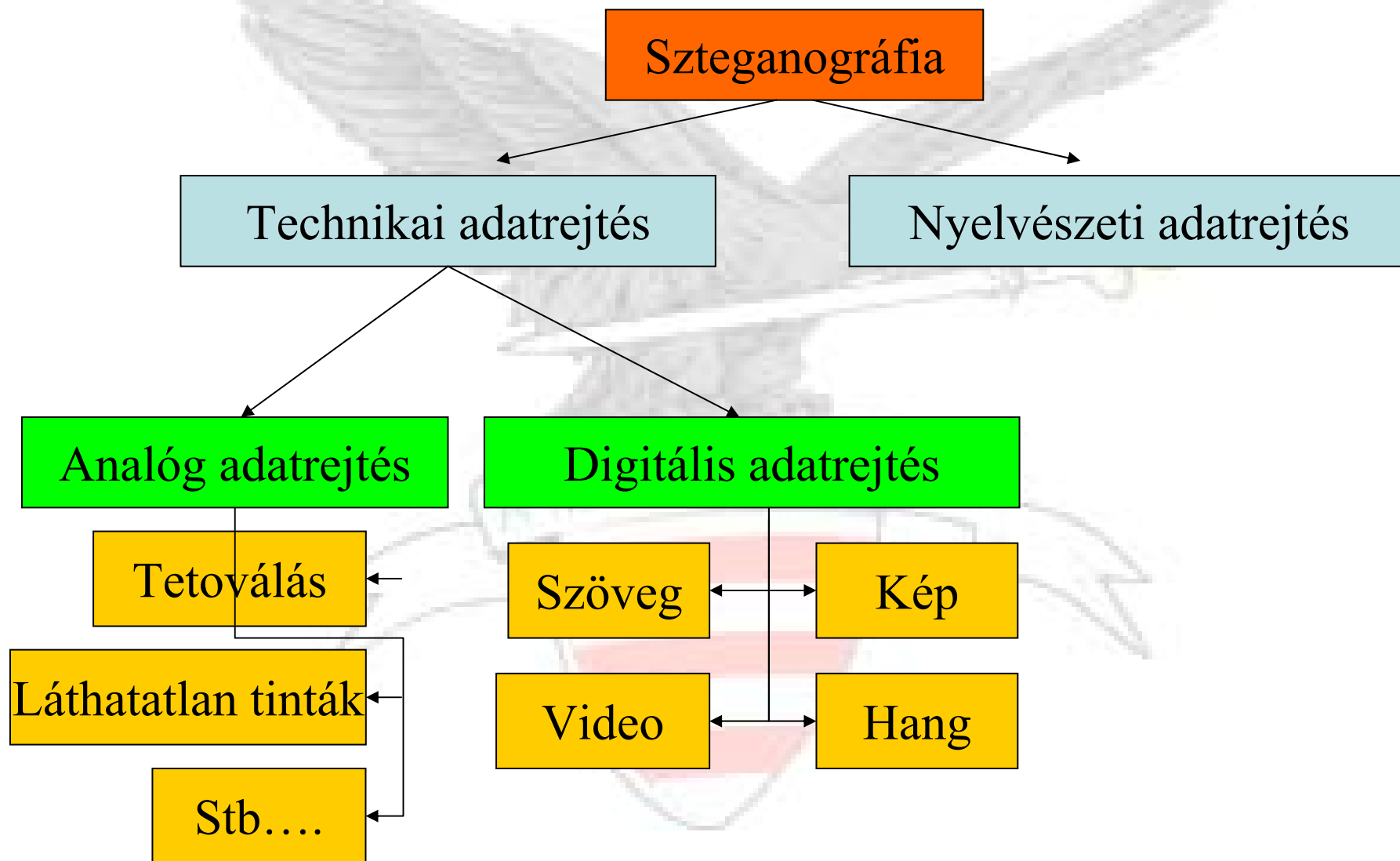
Szteganográfia jelentése és célja:

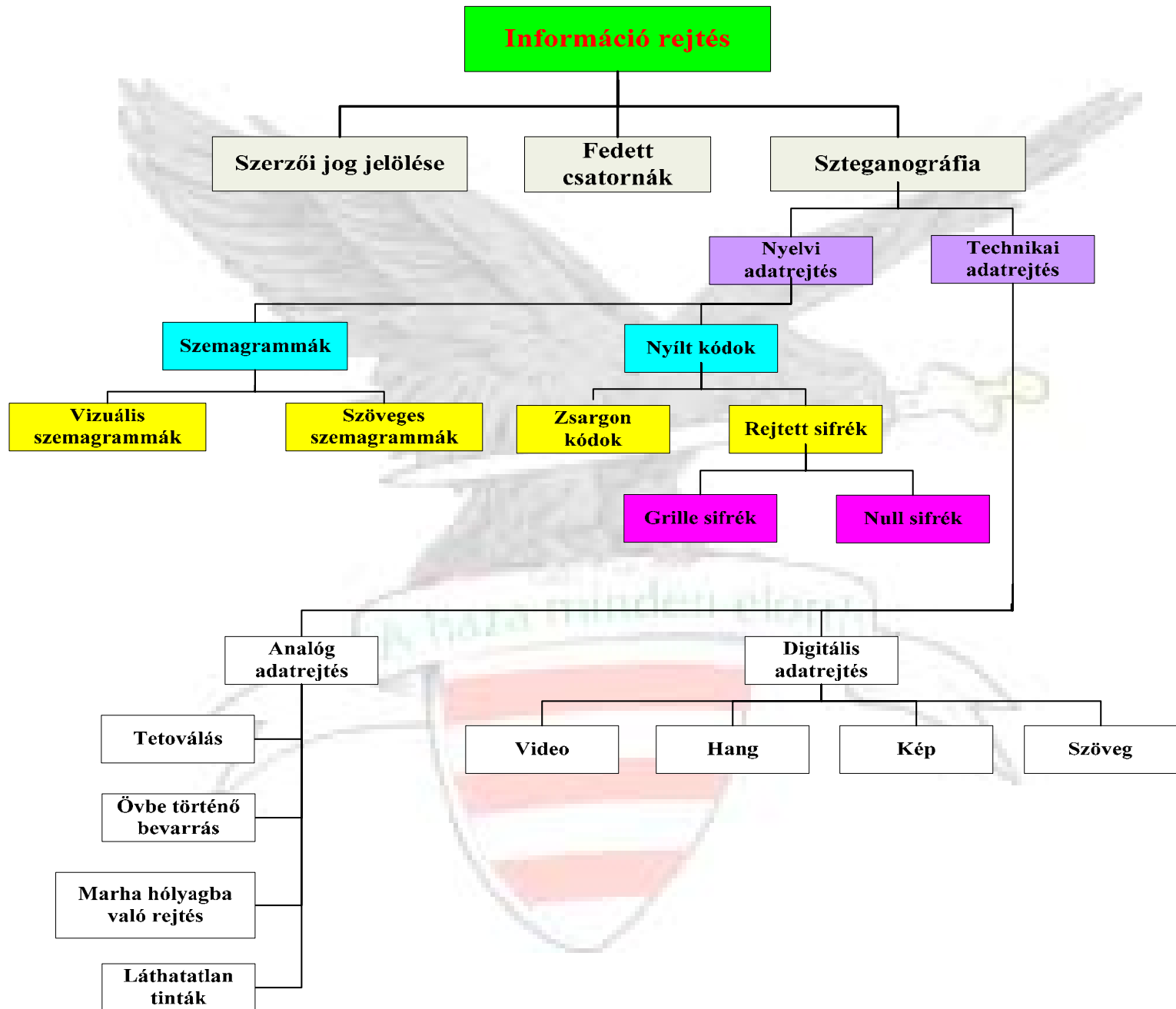
- Szteganográfia a rejtett, vagy fedett írás művészete. Célja a kommunikáció tényének elrejtése a harmadik fél előtt.

Szteganográfia fő csoportjai:



Szteganográfia felosztása folyt.





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.

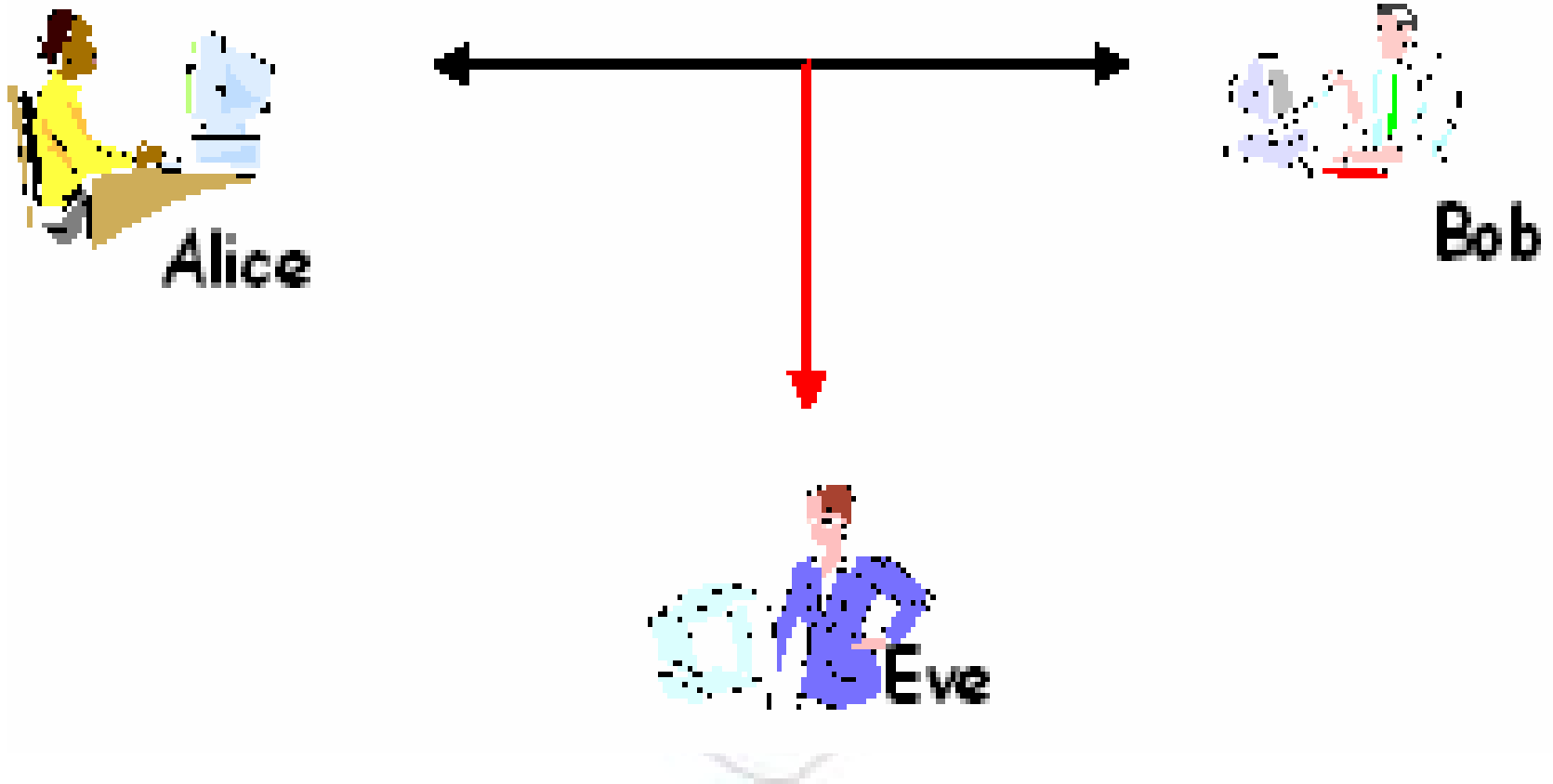
A szteganográfiai támadások célja.....

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.

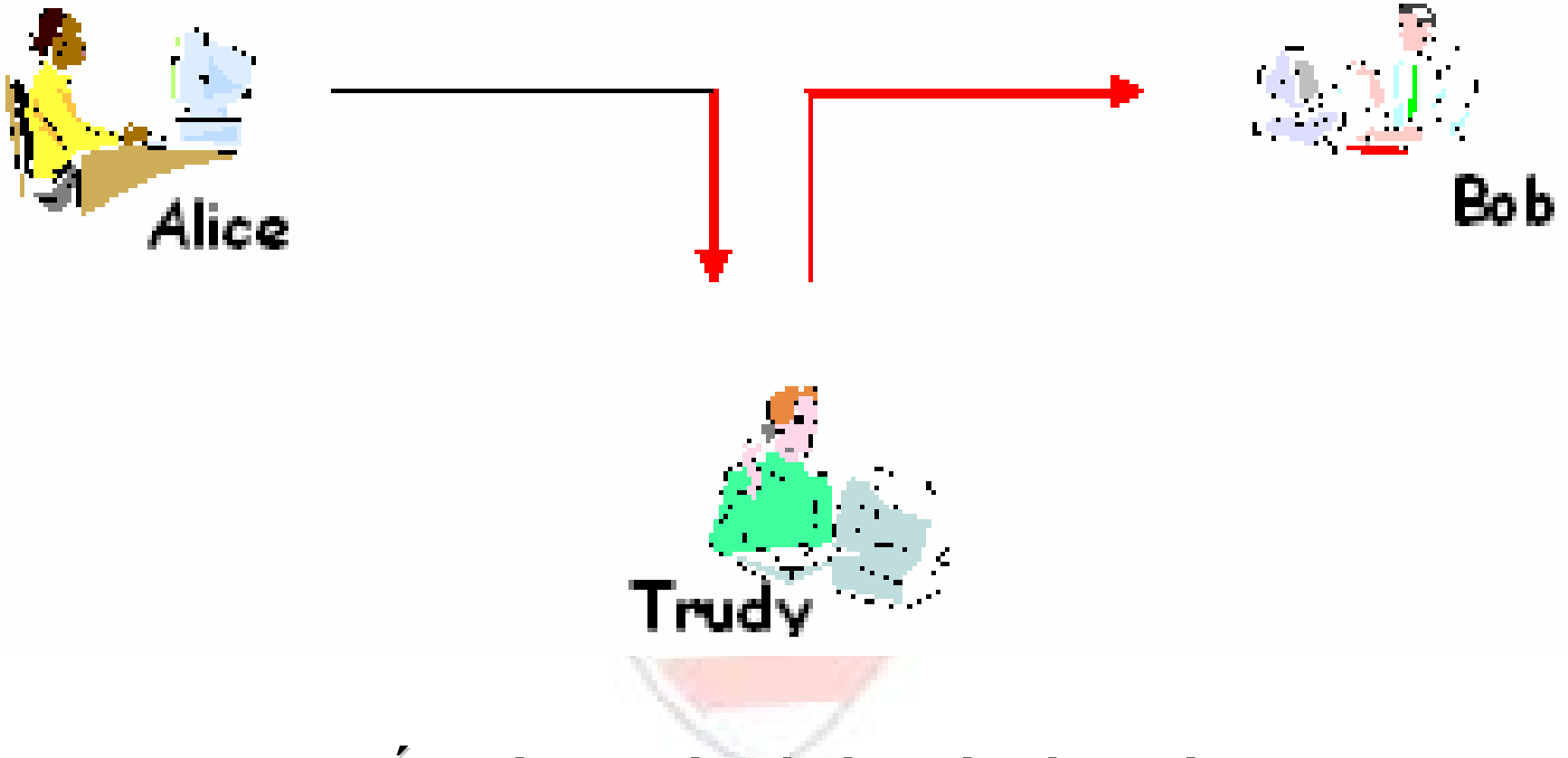
Fogvatartottak problémája.....

Passzív támadás:



Fogvatartottak problémája.....foyt.

Aktív támadások:



Általános szándékú aktív támadás

Fogvatartottak problémája.....foyt.



Alice



Bob

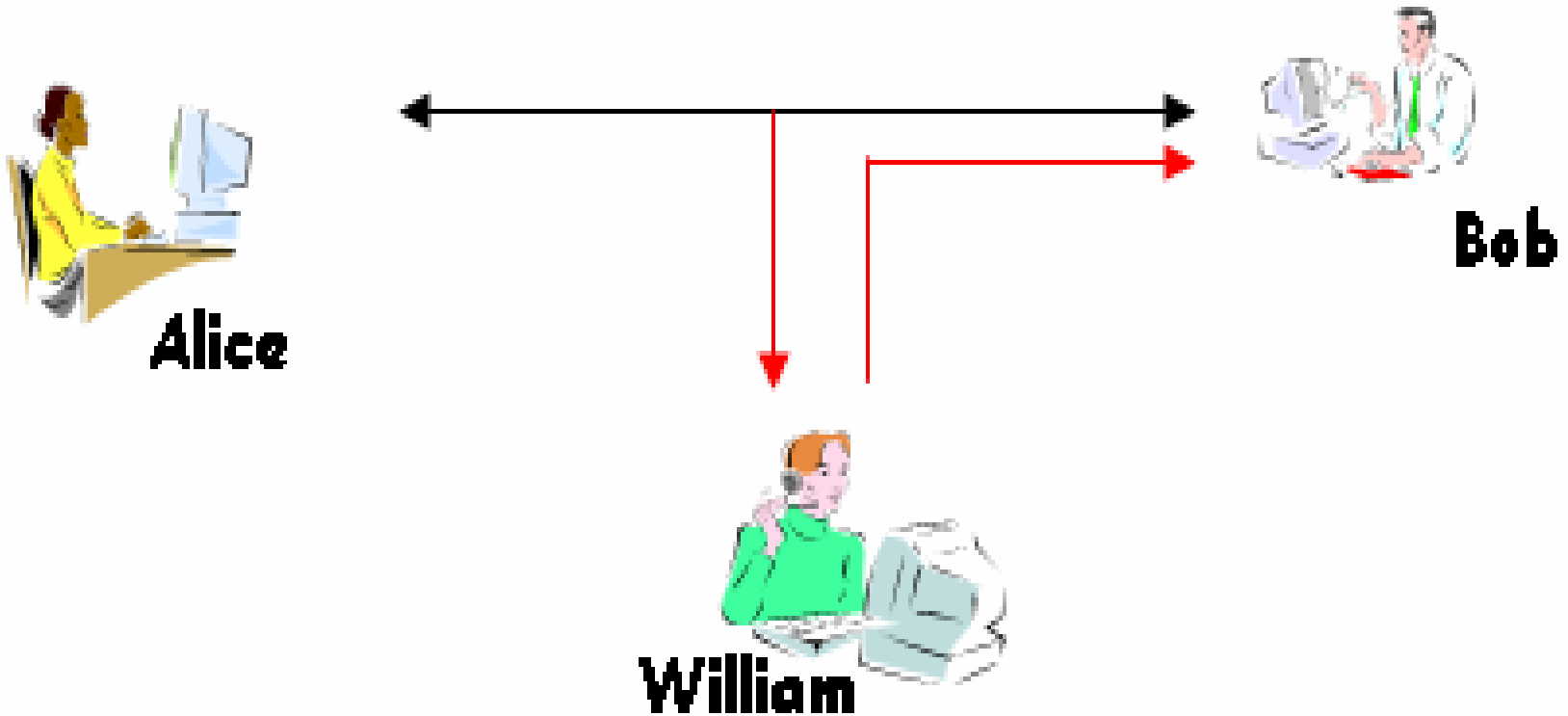


William



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.

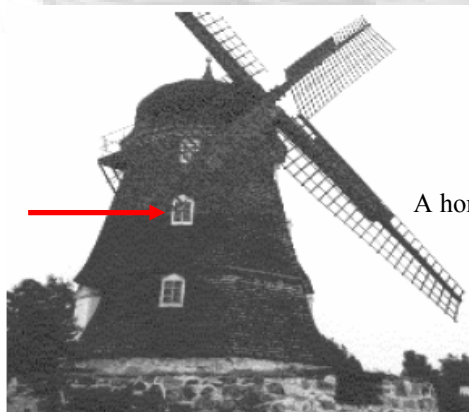
A detektálás osztályozása történhet:

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

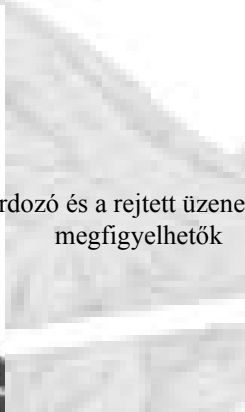


Szteganográfia Detektálhatósága folyt.

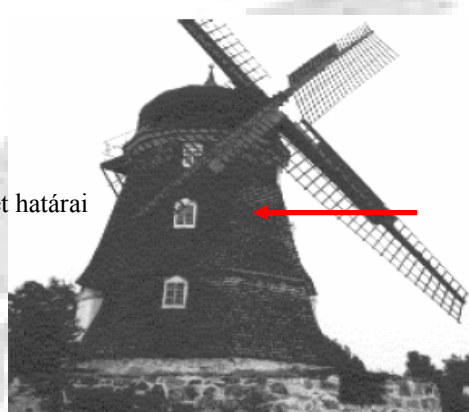
Vizuális támadások:



Eredeti hordozó



A hordozó és a rejtett üzenet határai megfigyelhetők

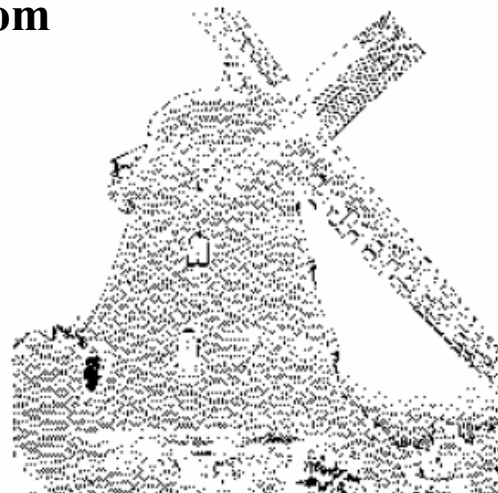


Rejtett üzenet

tartalom



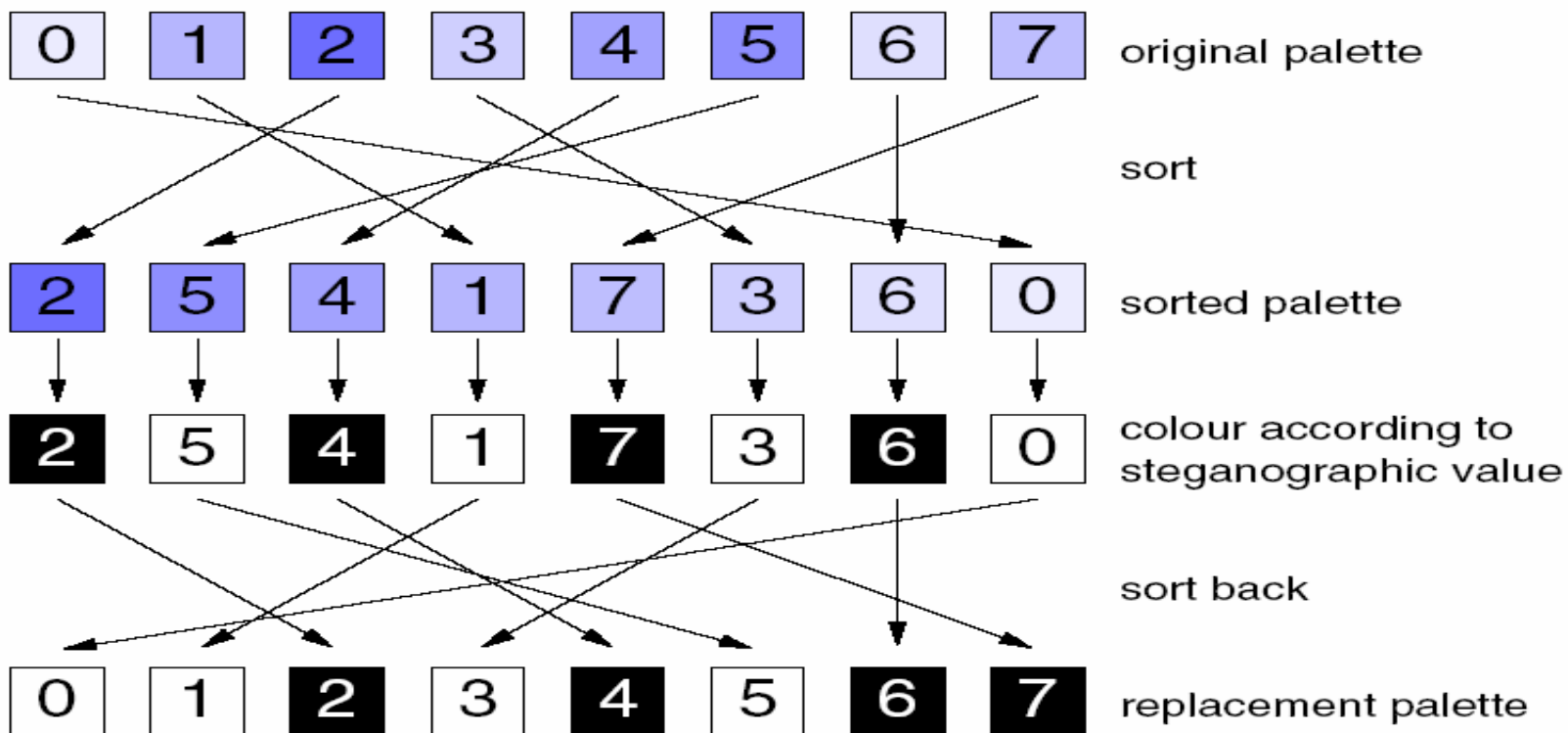
LSB=0 ha fekete



LSB=1 ha fehér

Szteganográfia Detektálhatósága folyt.

Vizuális támadások:



Szteganográfia Detektálhatósága folyt.

Vizuális támadások:



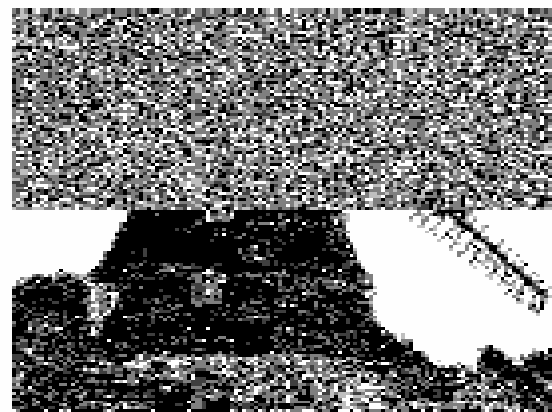
Eredeti hordozó



Rejtett üzenet



Szűrt A

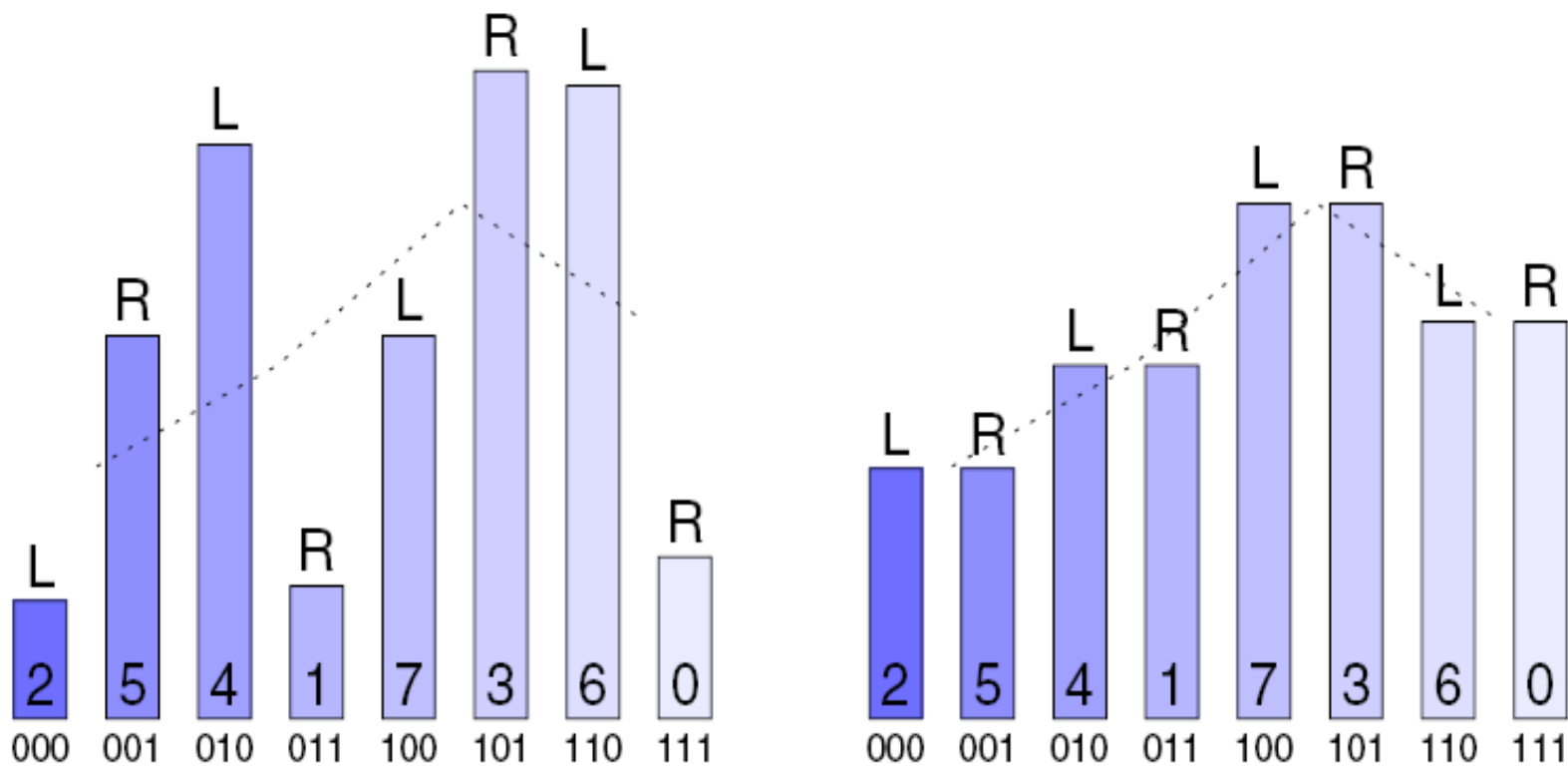


Szűrt B

Szteganográfia Detektálhatósága folyt.

Statisztikai támadások:

Chi-square Attack



A szteganalízis eszközei

A szteganográfia detektálására hivatott szoftvereket szteganalitikai eszközöknek hívjuk.

Néhány szabadon felhasználható, néhányuk fizetős és meglehetősen drága.

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

Néhány szteganalitikai szoftver:

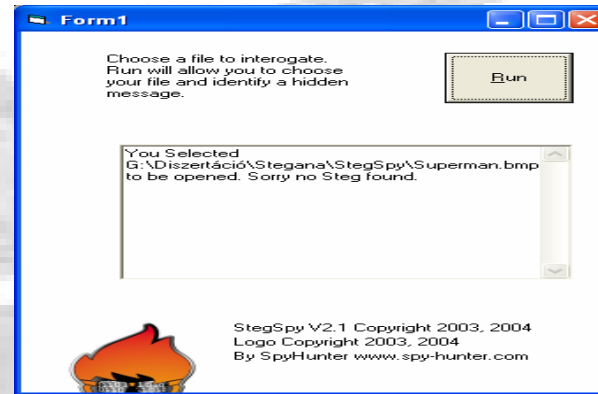
Szoftver neve	Detektált média	Licence	Fejlesztő/gyártó
StegSpy	JPEG	Szabadon felhasználható	Michael T. Raggo
Stegdetect	JPEG	Nyílt forrású	Niels Provos
StegBreak	JPEG	Nyílt forrású	Niels Provos
StegSuite		Licence díjas	Wetstone Technologies
StegAnalyzer	JPEG	Licence díjas	Wetstone Technologies

A szteganalízis eszközei folyt.

Stegspy:



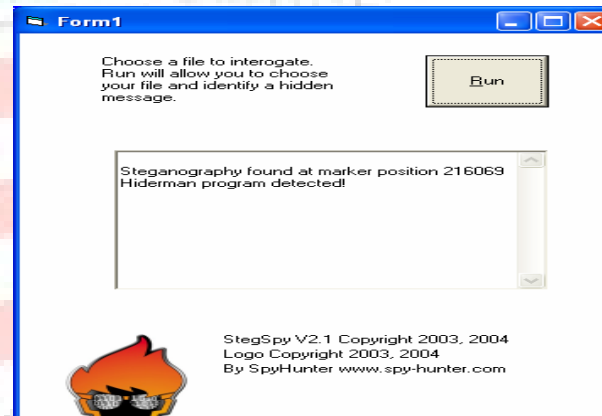
25/a Eredeti hordozó (1.1 MB)



25/b StegSpy analízis eredménye



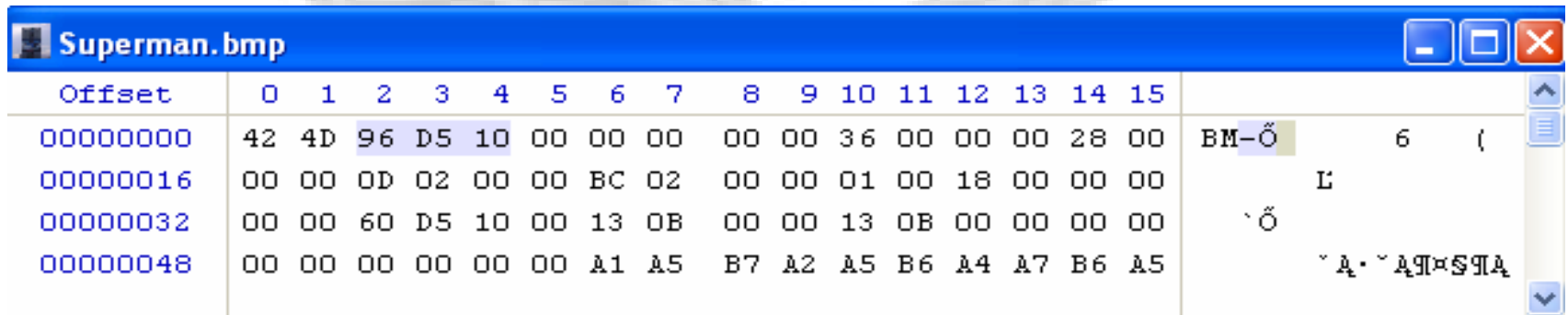
Beágyazott állományt tartalmazó hordozó (108,5 KB)



Beágyazott állomány a hordozóban, a 216069-os pozíciótól kezdődően

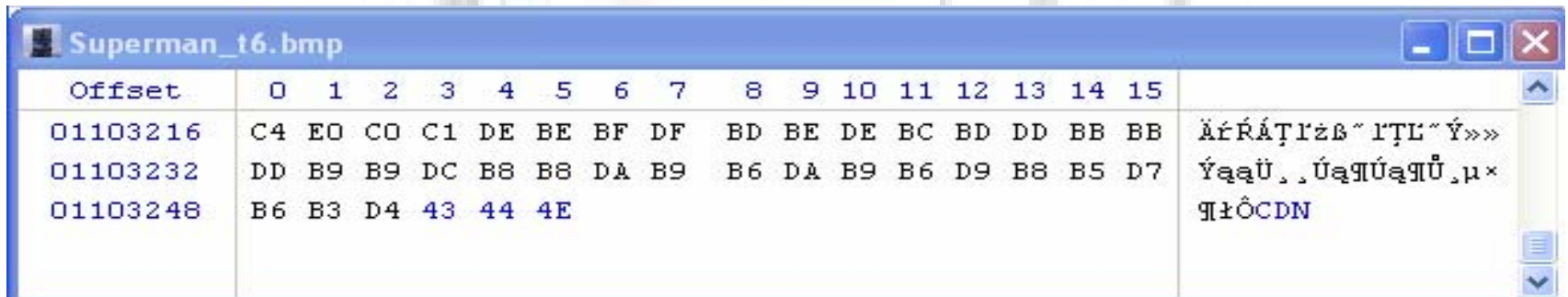
A szteganalízis eszközei folyt.

Stegspy:



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	42	4D	96	D5	10	00	00	00	00	00	36	00	00	00	28	00	BM-Ö 6 (
00000016	00	00	0D	02	00	00	BC	02	00	00	01	00	18	00	00	00	L
00000032	00	00	60	D5	10	00	13	0B	00	00	13	0B	00	00	00	00	`Ö
00000048	00	00	00	00	00	00	A1	A5	B7	A2	A5	B6	A4	A7	B6	A5	~A·~A¶×S¶A

A BMP fájl fejlécének kezdete

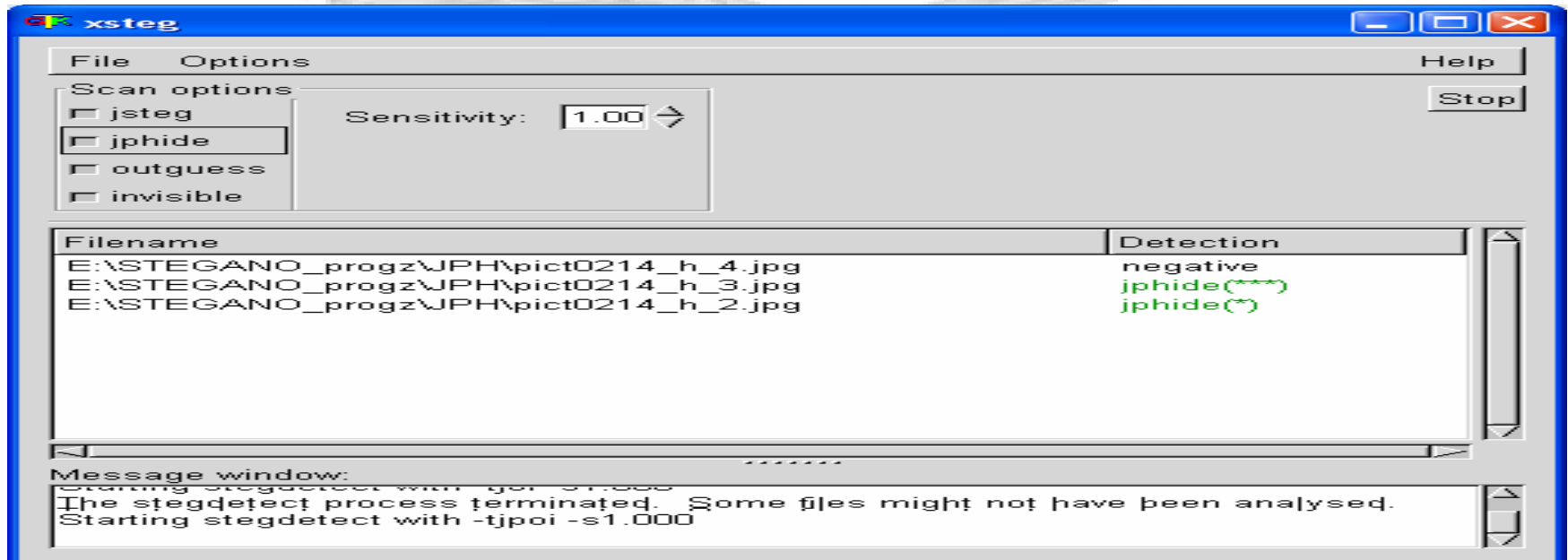


Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
01103216	C4	EO	CO	C1	DE	BE	BF	DF	BD	BE	DE	BC	BD	DD	BB	BB	ÄíRÁ¶IzB~I¶L~Ý»»
01103232	DD	B9	B9	DC	B8	B8	DA	B9	B6	DA	B9	B6	D9	B8	B5	D7	ÝaaÜ, .Úaa¶Úaa¶Ü,µ×
01103248	B6	B3	D4	43	44	4E											¶IÖCDN

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, amellet, hogy az AS modifikáció valamennyi képességével bír.

A szteganalízis eszközei folyt.

WinHex:

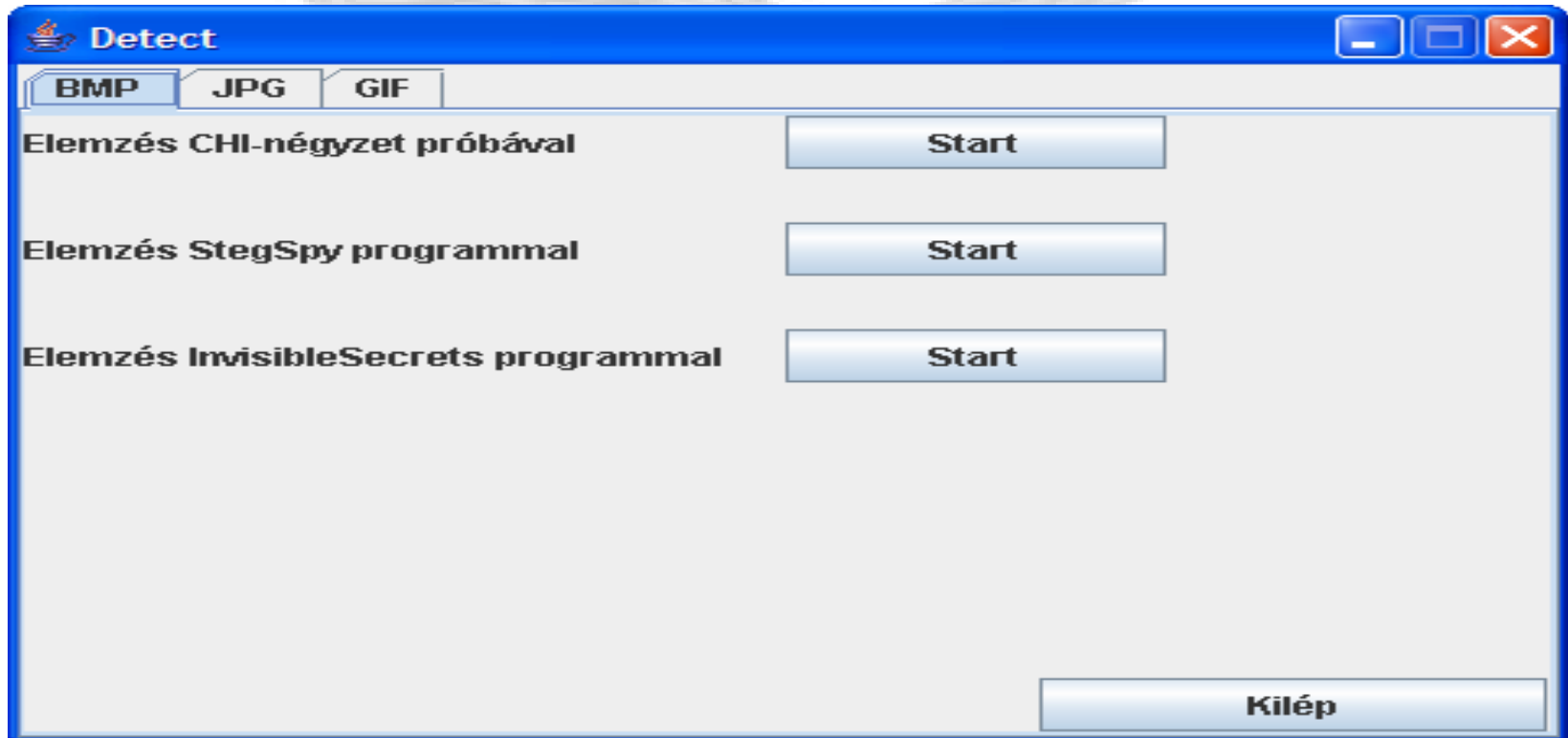
The screenshot shows the WinHex application interface. The main window displays the hex data of a file named PICT0525.JPG. The hex data is organized into columns labeled 0 through F, representing hexadecimal digits. The data is displayed in a grid format, with each row representing a line of hex data. The first dialog box, titled "MD5 (128 bit)", shows the MD5 hash for the selected data: D5EF5F3D17ACD4F52A57FE923B1B7781. The second dialog box, also titled "MD5 (128 bit)", shows the MD5 hash for a different selection: F798331820BD62F508AF189953484883. The status bar at the bottom indicates "Page 1 of 2422", "Offset: A5", "= 5 Block:", "n/a Size:", and "n/a".

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000070	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000080	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000090	01	01	01	01	01	01	01	01	01	01	01	01	01	01	FF	C0
000000A0	00	11	08	03	C0	05	00	03	01	21	00	02	11	01	03	11
000000B0	01	FF	C4	00	1F	00	00	01	04	03	01	01	01	01	00	00
000000C0	00	00	00	00	00	00	05	03	04	06	07	02	08	09	01	00
000000D0	0A	0B	FF	C4	00	4C	10	00	01	03	02	04	04	04	03	07
000000E0	04	02	01	03	01	01	11	01	02	03	11	04	21	00	05	12
000000F0	31	06	41	51	61	07	13	22	71	81	91	A1	08	14	32	B1
00000100	C1	D1	F0	23	42	E1	F1	09	15	52	16	24	33	62	43	72
00000110	17	25	82	18	34	92	0A	53	B2	C2	26	44	63	73	93	A2
00000120	FF	C4	00	1D	01	00	02	03	01	01	01	01	01	00	00	00
00000130	00	00	00	00	00	03	04	02	05	06	01	07	00	08	09	FF

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	FF	D8	FF	EO	00	10	4A	46	49	46	00	01	01	00	00	01
00000010	00	01	00	00	FF	DB	00	43	00	01	01	01	01	01	01	01
00000020	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000030	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000040	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000050	01	01	01	01	01	01	01	01	01	FF	DB	00	43	01	01	01
00000060	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000070	01	01	01	01	01	01	01	01	11	11	11	11	11	11	11	11
00000080	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01
00000090	01	01	01	01	01	01	01	01	01	01	01	01	01	01	FF	C0
000000A0	00	11	08	03	C0	05	00	03	01	21	00	02	11	01	03	11
000000B0	01	FF	C4	00	1F	00	00	01	04	03	01	01	01	01	00	00
000000C0	00	00	00	00	00	00	05	03	04	06	07	02	08	09	01	00

A szteganalízis eszközei folyt.

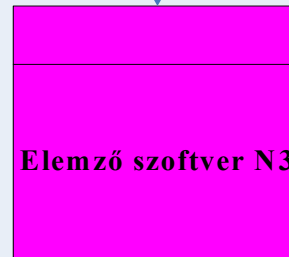
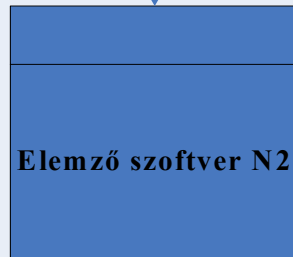
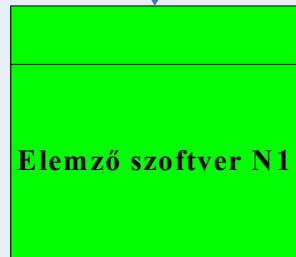
Detect:



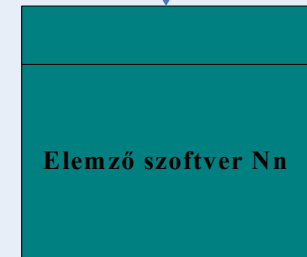
A szteganalízis eszközei folyt.

Detect:

Detect keretrendszer

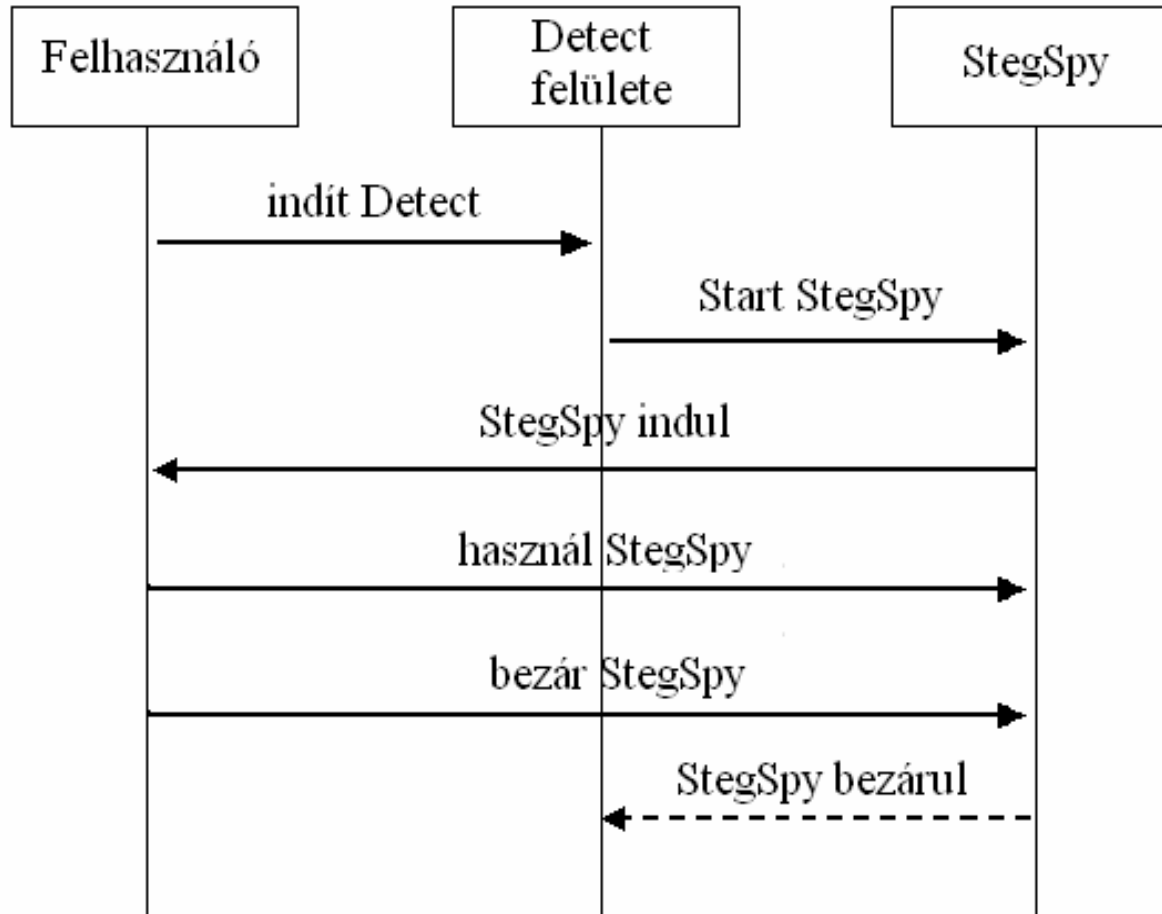


.....



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 paramétereinek 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

- **Relatív 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 kriptóanalízishez. Az előforduló gyenge pontok feltárására koncentrálnak.**
- **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 elérhető programok garmadája.
- Sokkal kevesebb publikált analitikai program, többségük borsos áron.
- 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>



Kérdések

Köszönöm, hogy meghallgattak!