

Estegoanálisis

Archivos de Prueba

Se cuenta con 4 archivos de prueba:

1. buenosaires.bmp
2. buenosaires0.bmp
3. topgun0.bmp
4. frozen.bmp

Condiciones Iniciales

Se conoce que los 4 archivos cuentan con algún tipo de información oculta. Además se sabe que hay un archivo utilizando LSB1, otro LSB4, otro LSBI y el último no utiliza una estenografía de tipo LSB.

Análisis

Para cada archivo se intenta abrirlo con todos los métodos de estenografía que no se hayan utilizado exitosamente todavía. Primero se prueba levantar todos los archivos sin ningún tipo de encriptación.

buenosaires.bmp

LSB1

```
./stegobmp --extract -p grupo20/buenosaires.bmp -o extracted_buenosaires --steg=LSB1
```

Utilizando LSB1 no se tuvo éxito.

LSB4

```
./stegobmp --extract -p grupo20/buenosaires.bmp -o extracted_buenosaires --steg=LSB4
```

Utilizando LSB4 sí se tuvo éxito y se encontró la siguiente imagen escondida:



buenosaires0.bmp

LSB1

```
./stegobmp --extract -p grupo20/buenosaires0.bmp -o extracted_buenosaires0 --steg=LSB1
```

Utilizando LSB1 no se tuvo éxito.

LSBI

```
./stegobmp --extract -p grupo20/buenosaires0.bmp -o extracted_buenosaires0 --steg=LSBI
```

Utilizando LSBI no se tuvo éxito.

Es posible que el archivo se encuentre encriptado, por lo que se continua con otro archivo.

topgun0.bmp

LSB1

```
./stegobmp --extract -p grupo20/topgun0.bmp -o extracted_topgun0 --steg=LSB1
```

Utilizando LSB1 no se tuvo éxito.

LSBI

```
./stegobmp --extract -p grupo20/topgun0.bmp -o extracted_topgun0 --steg=LSBI
```

Utilizando LSBI se obtuvo un archivo `extracted_topgun0.pdf` con el mensaje:

al .png cambiarle la extension por .zip y descomprimir

Parecería ser que se refiere al archivo que se obtuvo a partir de la imagen `buenosaires.bmp`

extracted_buenosaires0.png

Siguiendo las instrucciones del pdf anterior, se ejecuta lo siguiente:

```
cp extracted_buenosaires.png bsas.zip && unzip bsas.zip
```

y de esta manera se obtiene un archivo `sol20.txt` que dice lo siguiente:

cada mina es un 1. cada fila forma una letra. Los ascii de las letras empiezan todos en 01. Asi encontraras el algoritmo que tiene clave de 128 bits y el modo La password esta en otro archivo Con algoritmo, modo y password hay un .wmv encriptado y oculto.



								ASCII
0	1	0	0	0	0	0	1	A
0	1	1	0	0	1	0	1	E
0	1	1	1	0	0	1	1	S
0	1	0	0	0	1	0	1	E
0	1	1	0	0	0	1	1	C
0	1	1	0	0	0	1	0	B

Seguindo las instrucciones obtenemos que hay un archivo que está encriptado con AES128 y modo ECB. Además nos dicen que este archivo es un video (wmv).

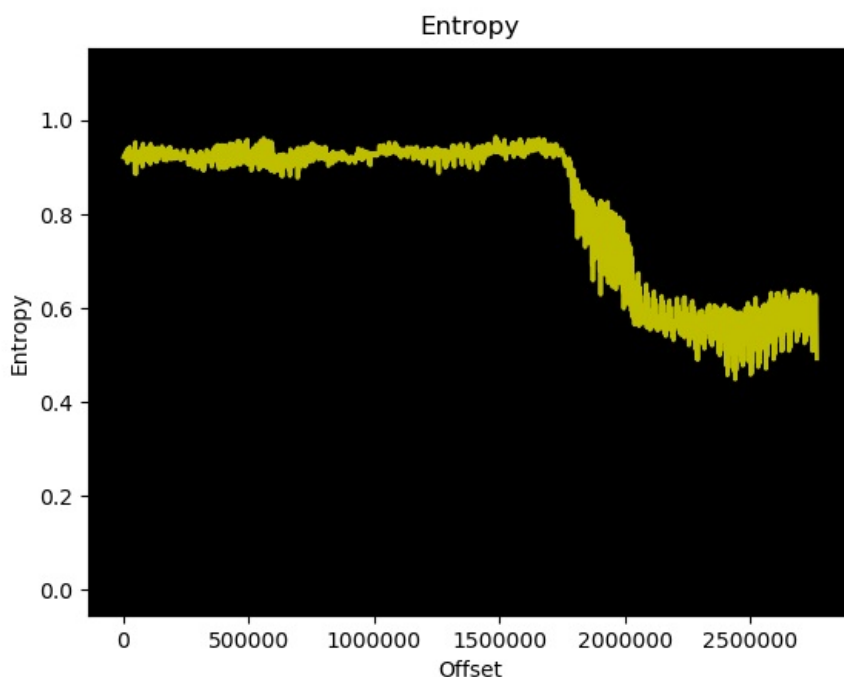
Teniendo en cuenta que el archivo frozen.bmp es **significativamente** más grande que los demás, se sospecha que este es el archivo encriptado que contiene el video. Por lo tanto es probable que el archivo buenosaires0.bmp sea el que no contiene un mensaje utilizando un método LSB y por lo tanto sería el que contiene la contraseña como indica sol20.txt .

buenosaires0.bmp (devuelta)

Para investigar que podría estar pasando en este archivo se utilizó binwalk para ver la entropía del archivo y generar un gráfico correspondiente:

```
binwalk -E -J grupo20/buenosaires0.bmp
```

Con esto obtenemos el siguiente gráfico:



Parecería indicar que puede llegar a haber información al final del archivo.

Abriéndolo con un hexeditor se encuentra lo siguiente:

buenosaires0.bmp

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
002A2EC0	96	69	D9	96	69	D9	96	69	D7	94	67	D6	93	66	D8	95	-iÿ-iÿ-i×"gø"fø•
002A2ED0	68	D7	94	67	D6	93	66	D6	93	66	D6	93	66	D7	94	67	h×"gø"fø"fø"f×"g
002A2EE0	D8	95	68	D8	95	68	D9	95	68	D8	94	67	D7	93	66	D7	ø•hø•hÿ•hø"g×"f×
002A2EF0	93	66	D8	94	67	D9	95	68	D8	95	68	D8	95	68	D8	95	"fø"gÿ•hø•hø•hø•
002A2F00	68	D8	95	68	D8	96	66	D8	96	66	D9	97	67	D9	97	67	hø•hø-fø-fÿ-gÿ-g
002A2F10	D9	97	67	D7	96	69	D6	95	69	D4	94	6B	D6	94	6B	D6	ÿ-g×-iø•iø"kø"kø
002A2F20	94	6B	D6	94	6B	D6	94	6B	D6	95	69	D6	95	69	D5	94	"kø"kø"kø•iø•iø"
002A2F30	68	D6	95	69	D8	95	68	D9	96	69	D9	96	69	D9	96	69	hø•iø•hÿ-iÿ-iÿ-i
002A2F40	D9	96	69	D8	95	68	D8	95	68	D8	95	68	D8	95	68	D8	ÿ-iø•hø•hø•hø•hø
002A2F50	95	68	D7	94	67	D8	95	68	D9	96	69	DA	97	6A	D9	96	•h×"gø•hÿ-iÿ-jÿ-
002A2F60	69	D8	95	68	D7	94	67	D7	94	67	D8	95	68	D9	96	69	iø•h×"g×"gø•hÿ-i
002A2F70	DA	97	6A	DA	97	6A	DA	97	6A	D9	96	69	D9	96	69	D9	ÿ-jÿ-jÿ-jÿ-jÿ-iÿ-iÿ
002A2F80	96	69	D9	96	69	D9	96	69	D9	96	69	D9	96	69	D9	96	-iÿ-iÿ-iÿ-iÿ-iÿ-iÿ-
002A2F90	69	D9	96	69	D9	96	69	DA	97	6A	D9	96	69	D9	96	69	iÿ-iÿ-iÿ-jÿ-iÿ-i
002A2FA0	D8	95	68	D6	95	69	D8	96	6D	D6	95	6E	D6	95	6E	D6	ø•hø•iø-mø•nø•nø
002A2FB0	95	6E	D6	96	6D	D6	96	6D	D8	96	6D	D8	96	6D	D7	95	•nø-mø-mø-mø-m×•
002A2FC0	6C	D6	94	6B	D5	94	68	D5	94	68	D7	93	68	D8	94	69	lø"kø"hø"h×"hø"i
002A2FD0	DA	96	6B	DB	97	6C	DB	98	6B	DA	97	6A	D9	96	69	D8	ÿ-kø-lÿ~kÿ-jÿ-iø
002A2FE0	95	68	D8	95	68	D9	96	69	D8	97	6B	D8	97	6B	D9	98	•hø•hÿ-iø-kø-kÿ~
002A2FF0	6C	D9	98	6C	D9	98	6C	D9	98	6C	D7	97	6E	D7	97	6E	lÿ~lÿ~lÿ~l×-n×-n
002A3000	D7	97	6E	D7	97	6E	D8	98	6F	D8	98	6F	D8	98	6F	D7	×-n×-nø~øø~øø~ox
002A3010	97	6E	D7	97	6E	D7	97	6E	D6	96	6D	D6	96	6D	D6	96	-n×-n×-nø-mø-mø-
002A3020	6D	D6	96	6D	D7	97	6E	D7	97	6E	D7	97	6E	D7	97	6E	mø-m×-n×-n×-n×-n
002A3030	D7	97	6E	D6	96	6D	6C	61	20	70	61	73	73	77	6F	72	×-nø-mla passwor
002A3040	64	20	65	73	20	64	65	73	61	66	69	61	72				d es desafiar

Special editors

Data inspector

Binary (8 bit)	01000010
Int8	66
UInt8	66
Int16	19778
UInt16	19778
Int24	3558722
UInt24	3558722
Int32	808865090
UInt32	808865090
Int64	181197491522
UInt64	181197491522
LEB128	-62
ULEB128	66
AnsiChar / char8_t	B
WideChar / char16_t	䄂
UTF-8 code point	B (U+0042)
Single (float32)	6.63210042439744E-10
Double (float64)	8.95234556736307E-313
CLOCKTIME	30/12/1899
FILETIME	1/1/1601 05:01:59
DOS date	2/10/2018
DOS time	09:42:04
DOS time & date	22/1/2004 09:42:04
time_t (32 bit)	18/8/1995 20:44:50
time_t (64 bit)	3/12/7711 04:32:02
GUID	{03964D42-002A-0000-0000-3600}
Disassembly (x86-16)	inc dx
Disassembly (x86-32)	inc edx
Disassembly (x86-64)	Invalid

Se puede ver que al final del archivo dice:

la password es desafiar

Teniendo en cuenta esto usamos las configuraciones obtenidas previamente para extraer el archivo de `frozen.bmp`.

frozen.bmp

Como ya se encontró un archivo con LSB4 y otro con LSBI este debería ser LSB1, encriptado utilizando AES128 en modo ECB con contraseña: desafiar

Corriendo lo siguiente:

```
./stegobmp --extract -p grupo20/frozen.bmp -o extracted_frozen \  
--steg=LSB1 -a=AES128 -m=ECB --pass=desafiar
```

Obtenemos el archivo `extracted_frozen.wmv` que es un video de 53s de una escena de la película Wanted (2008).