

Actividad 4 - Seguridad en Redes

Profesor: René Guerrero Torres

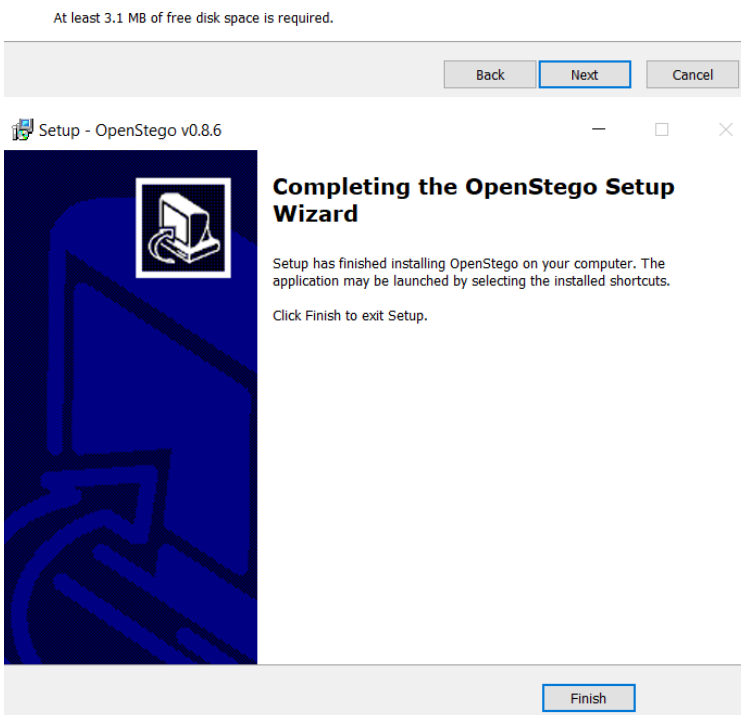
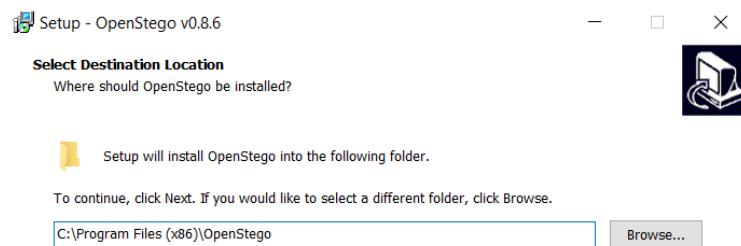
Ayudante: Iván Zuñiga

Alumno: Reinaldo Pacheco Parra

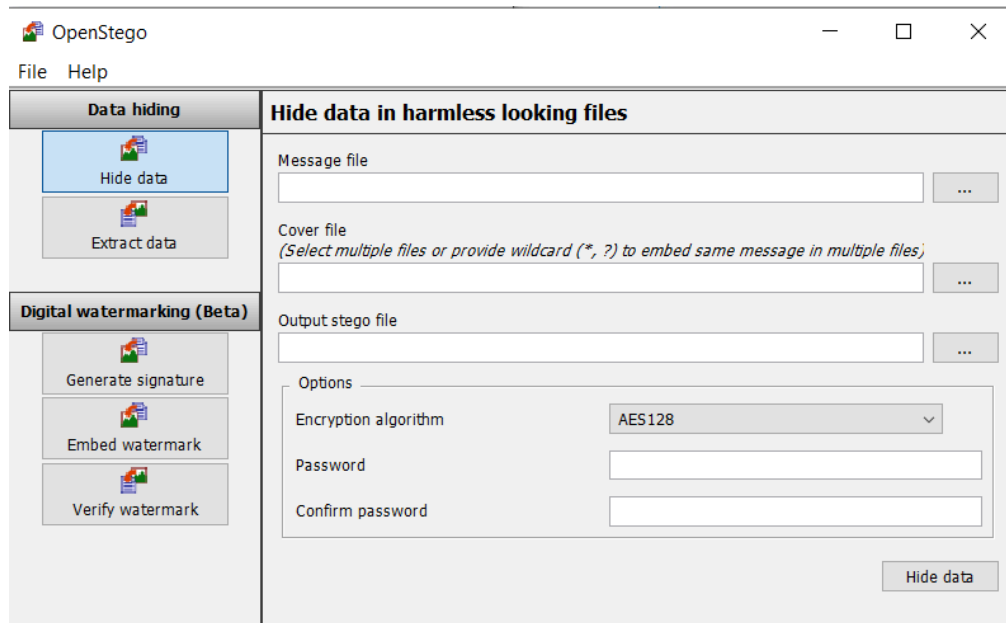
Actividad 4.1: Esteganografía en imagen y audio con OpenStego, DeepSound y Steghide

I.- OpenStego: Esteganografía en imagen

1. Se baja la aplicación OpenStego en la máquina Windows en el siguiente enlace:
<https://github.com/syvaidya/openstego/releases>
2. Se realiza la instalación de la aplicación



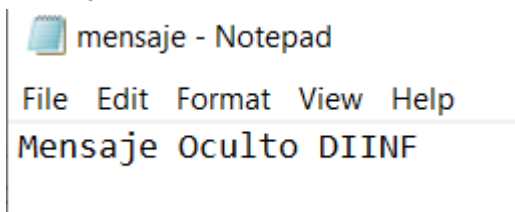
3. Se ejecuta la aplicación OpenStego

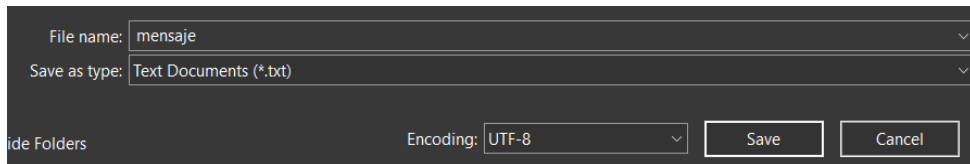


4. Se baja un archivo de imagen en formato jpg

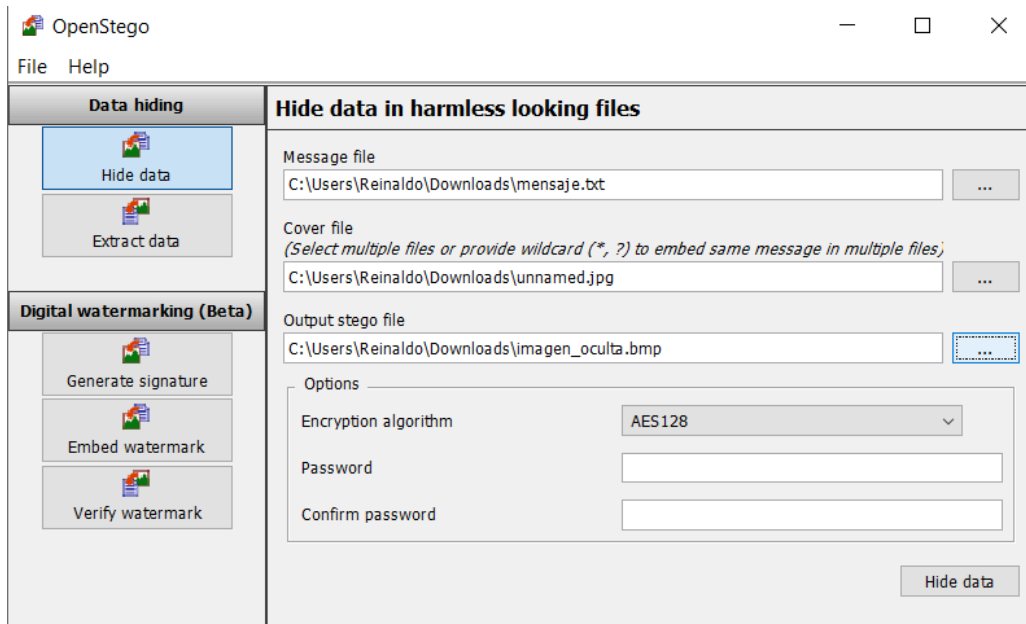


5. Se crea un archivo de texto con la aplicación Notepad y se guarda el archivo como mensaje.txt

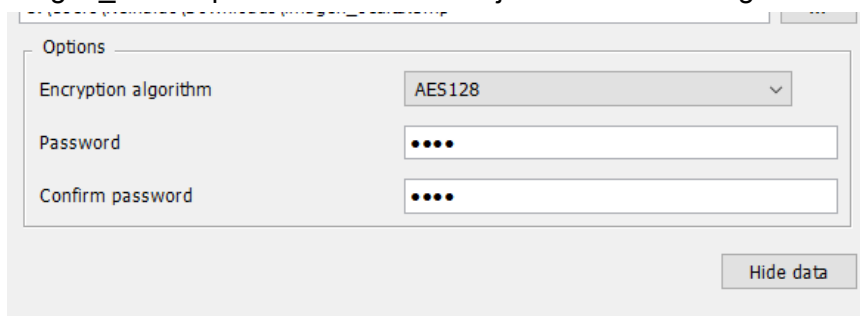




- Se carga el archivo de texto y la imagen en la aplicación, luego se selecciona como output el nombre del archivo de salida y la ubicación donde se guardará.

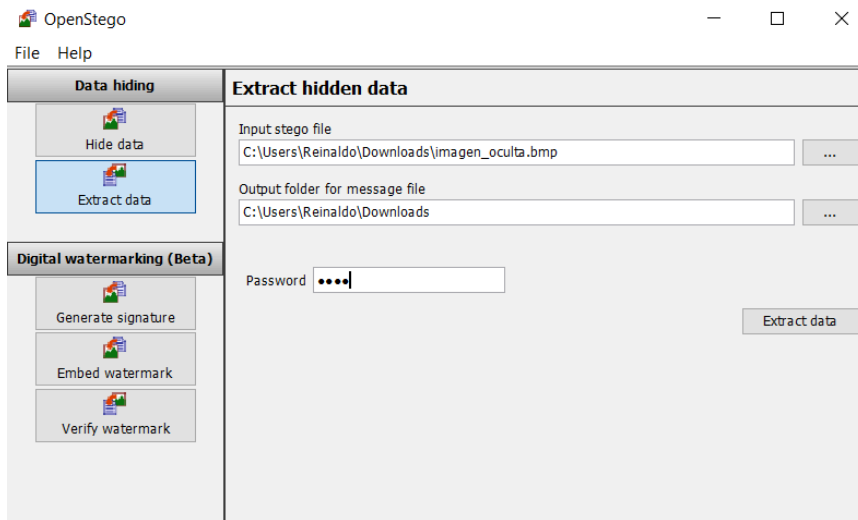


- Se selecciona el método de encriptación y una clave para guardar el archivo imagen_oculta que contiene el mensaje dentro de la imagen

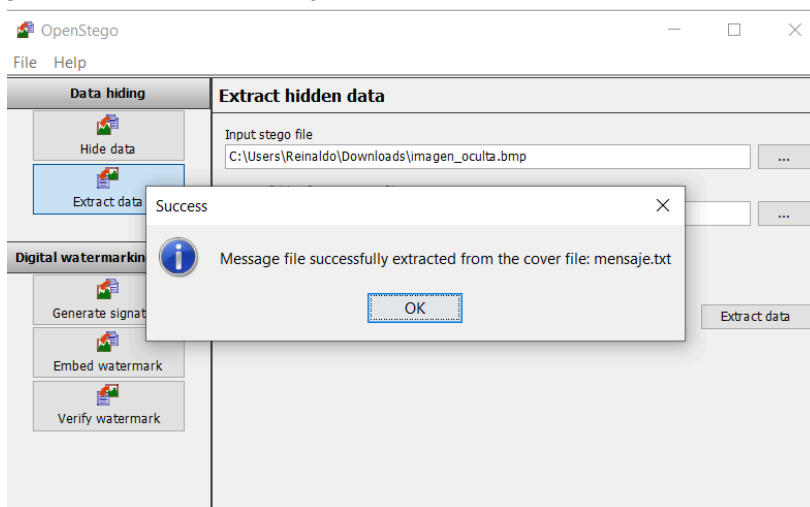


Name	Date modified	Type	Size
Today (8)			
imagen_oculta	11/19/2024 3:02 PM	BMP File	2,374 KB

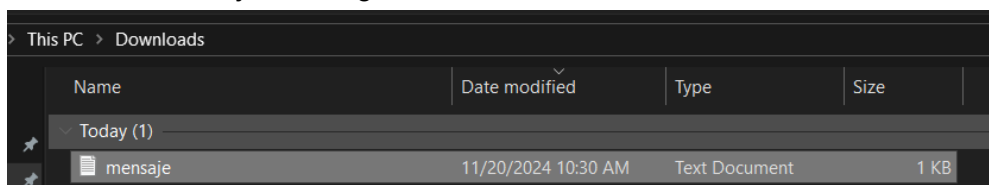
- Se borra el archivo de mensaje y se extrae la información de la imagen_oculta en la opción de Extract hidden data. Se ingresa el archivo de entrada (imagen_oculta), el directorio en donde se va a almacenar el mensaje de salida y la contraseña establecida anteriormente.



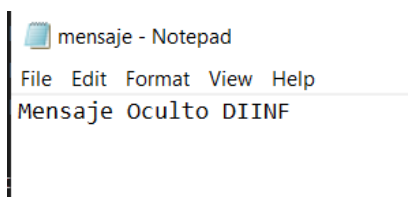
9. Luego, se presiona en Extract data para obtener los datos ocultos (mensaje.txt)
Se muestra un aviso que indica que se pudo extraer el mensaje oculto y que fue guardado como “mensaje.txt”



El archivo “mensaje.txt” se guarda correctamente en el directorio establecido

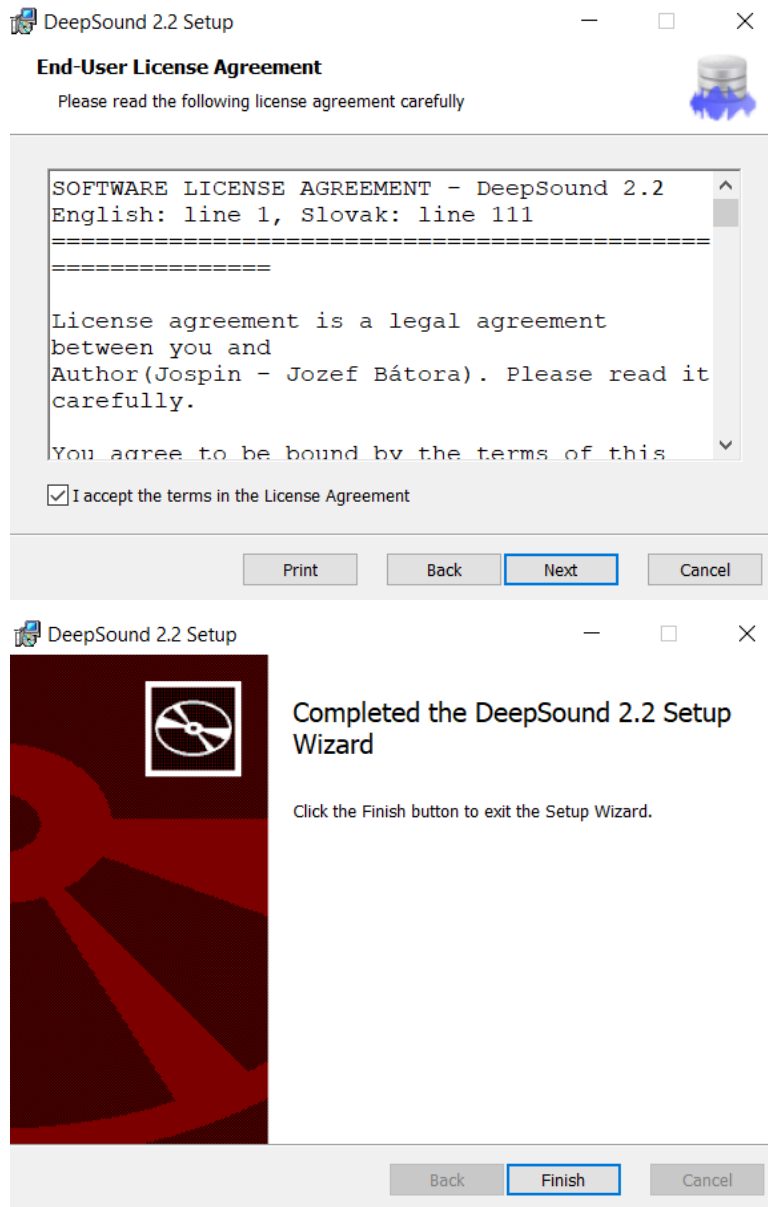


10. Se revisa el contenido del archivo resultante el cual es el mismo que se guardó

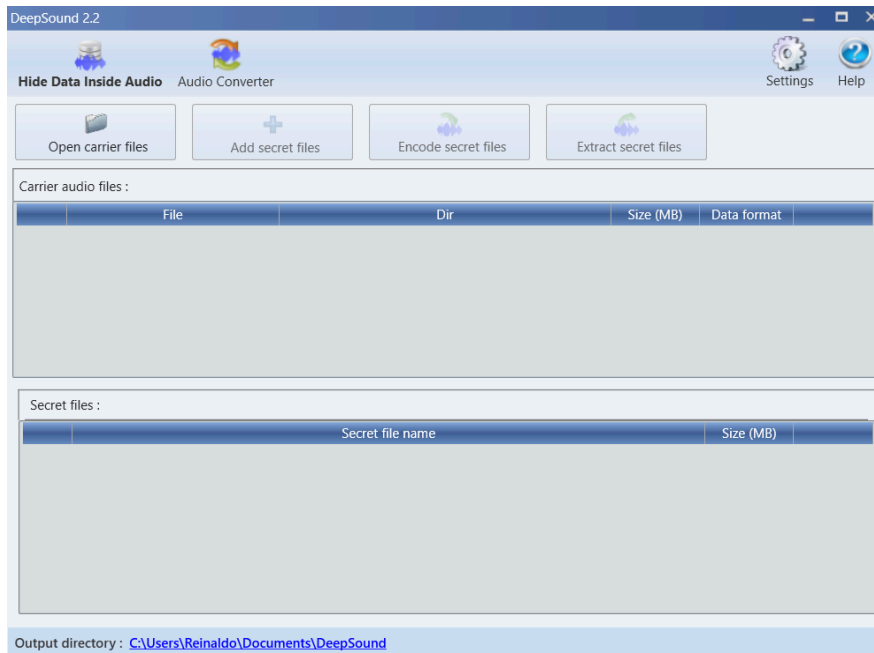


J.- Esteganografía de audio con DeepSound

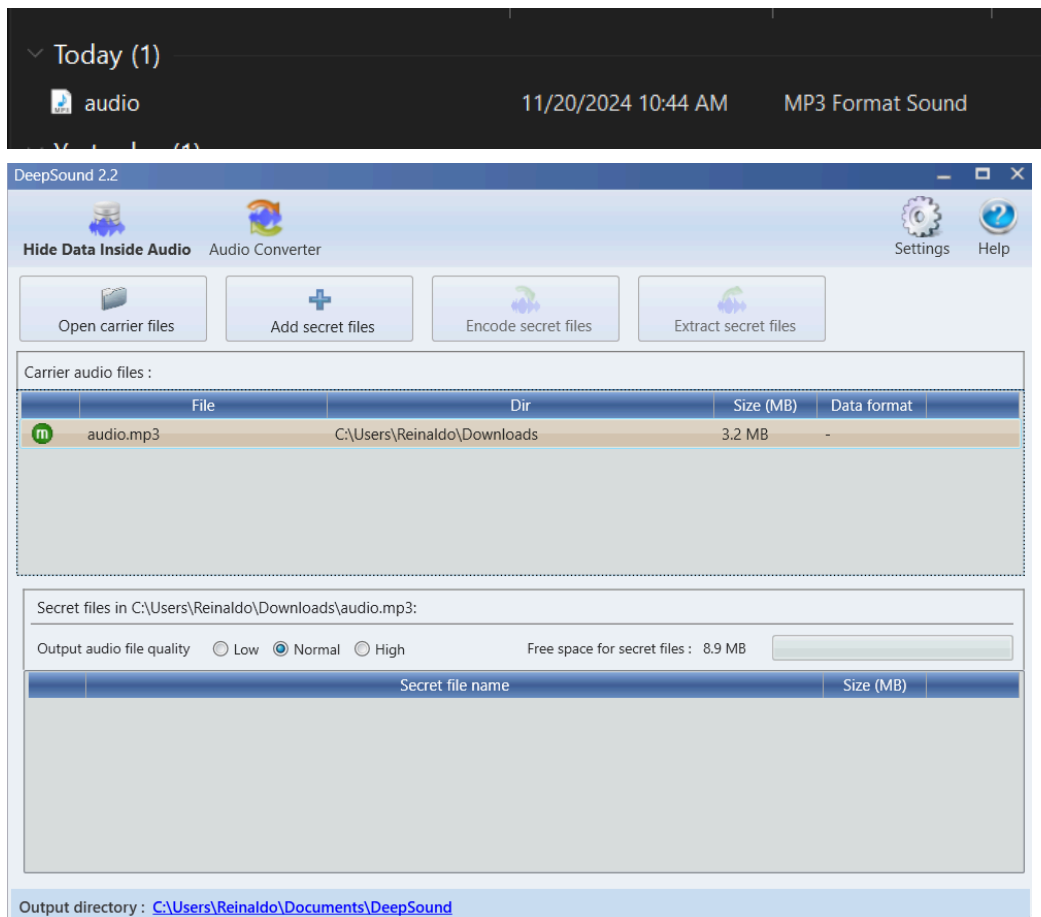
1. Se baja la aplicación DeepSound en la máquina Windows desde el enlace:
<https://github.com/Jpinsoft/DeepSound>
2. Se procede a la instalación de la aplicación



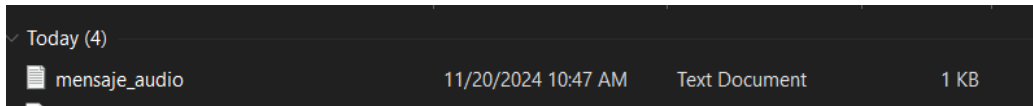
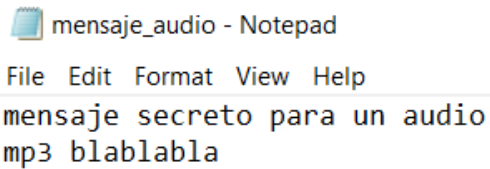
3. Se ejecuta la aplicación



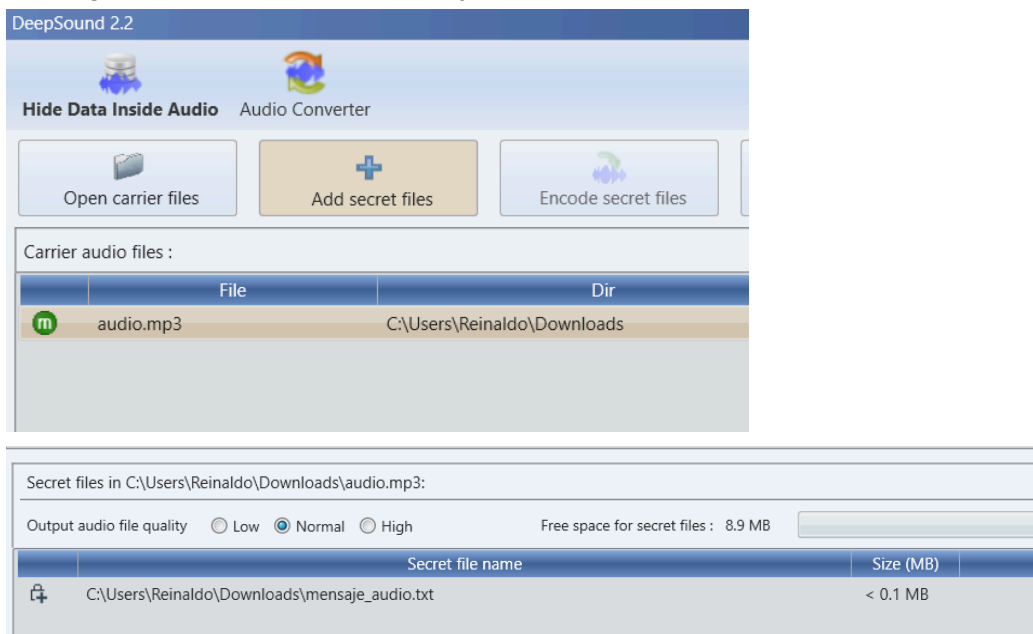
4. Se carga un archivo de audio en formato .mp3 en la sección de “Open carrier files”



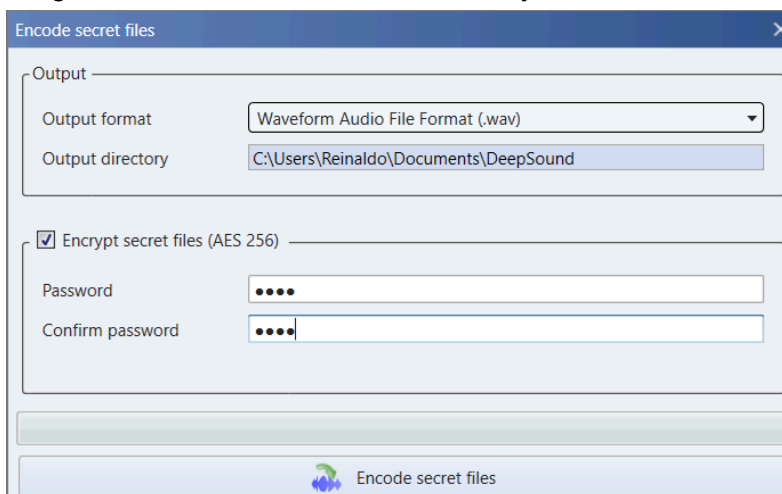
5. Se crea un archivo de texto con un mensaje secreto, se guarda como mensaje_audio.txt



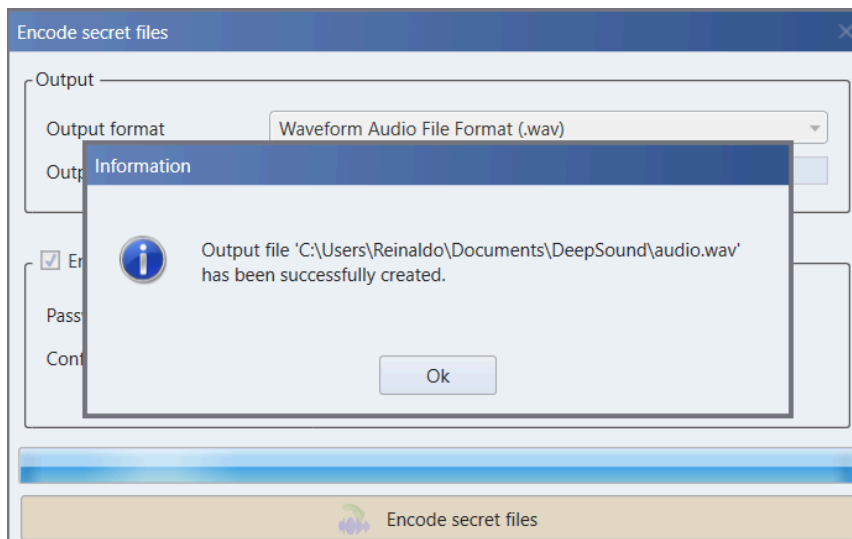
6. Se carga el archivo de texto mensaje_audio.txt en la opción “Add secret files”



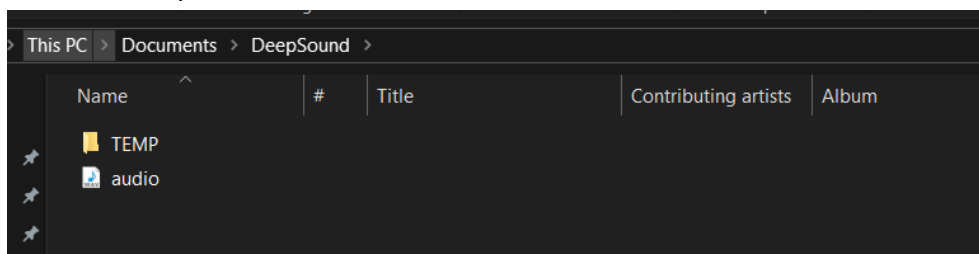
7. Se ejecuta la opción “Encode secret files” para cifrar el mensaje, se selecciona como formato de salida el archivo .wav y el directorio en donde se guardará el archivo. Luego se selecciona el cifrado AES256 y se establece una contraseña



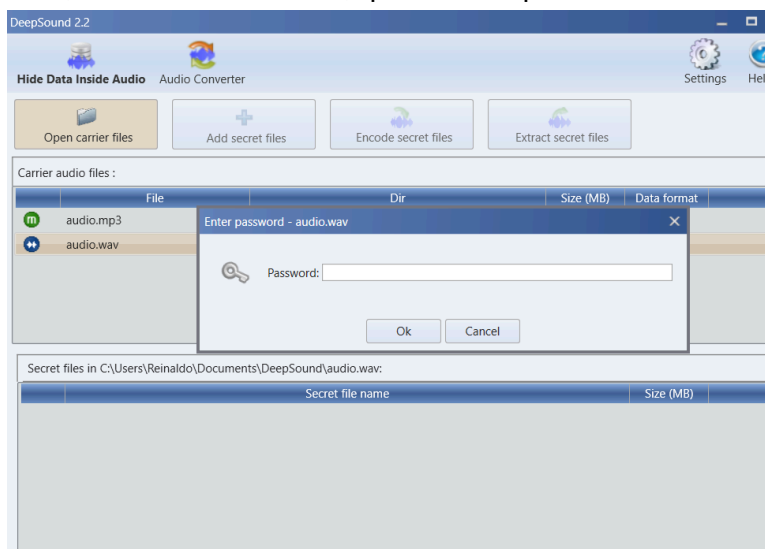
8. Se selecciona la opción “Encode secret files” para cifrar el mensaje. Se obtiene un aviso de que el archivo se creó correctamente.



9. Se confirma que el archivo se creó correctamente



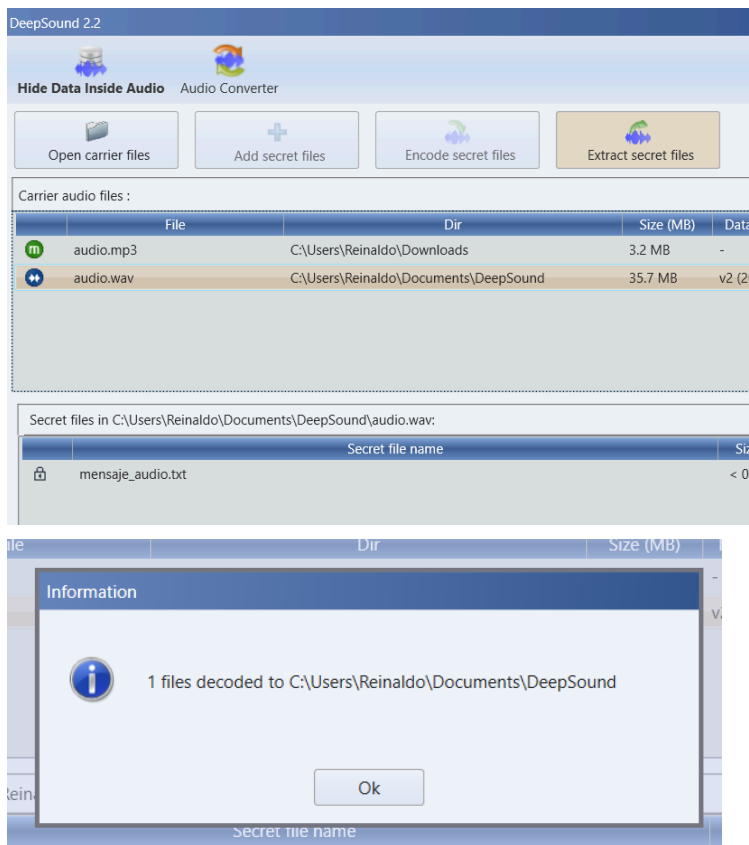
10. Luego, se carga el archivo generado recientemente en la sección “Open carrier files”, se solicita una clave, que será la que se estableció anteriormente.



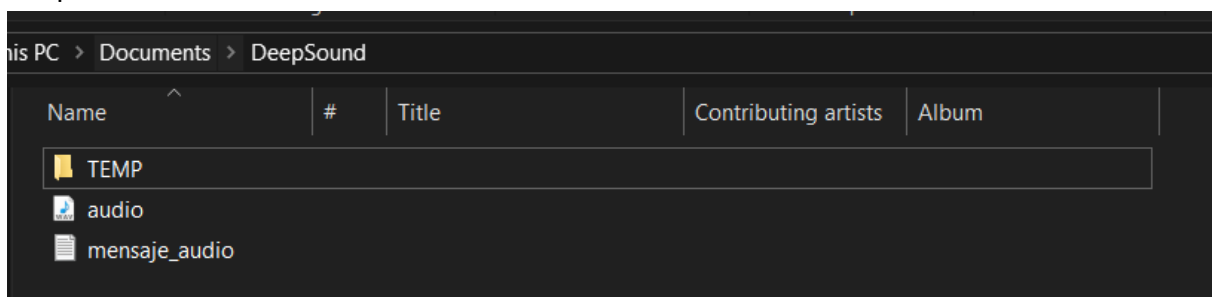
11. Se ingresa la contraseña y se puede visualizar en la sección “Secret files” que existen archivos secretos en el archivo subido.

Secret files in C:\Users\Reinaldo\Documents\DeepSound\audio.wav:		
	Secret file name	Size (MB)
🔒	mensaje_audio.txt	< 0.1 MB

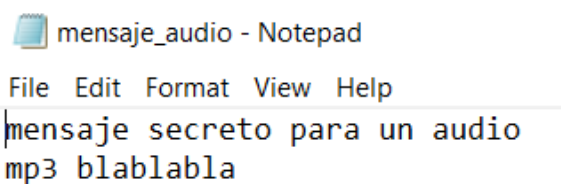
12. Se selecciona la opción “Extract secret files” para obtener los archivos secretos



13. Luego, se visualiza el archivo generado mensaje_audio en el directorio de Deepsound



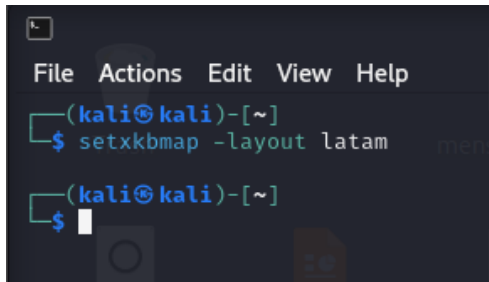
14. Se abre el archivo para verificar que es correcto.



E.- Uso de Steghide: Esteganografía en imagen

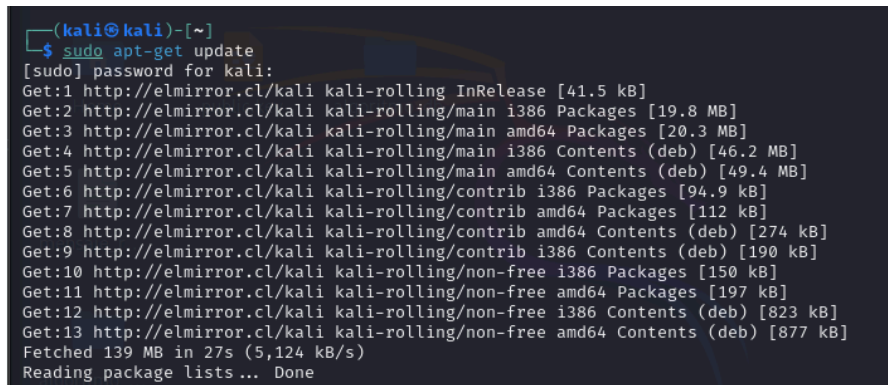
1. Se inicia la máquina Kali con la interfaz de red en modo NAT
2. Se configura el teclado en formato latam con el comando:

`setxkbmap -layout latam`



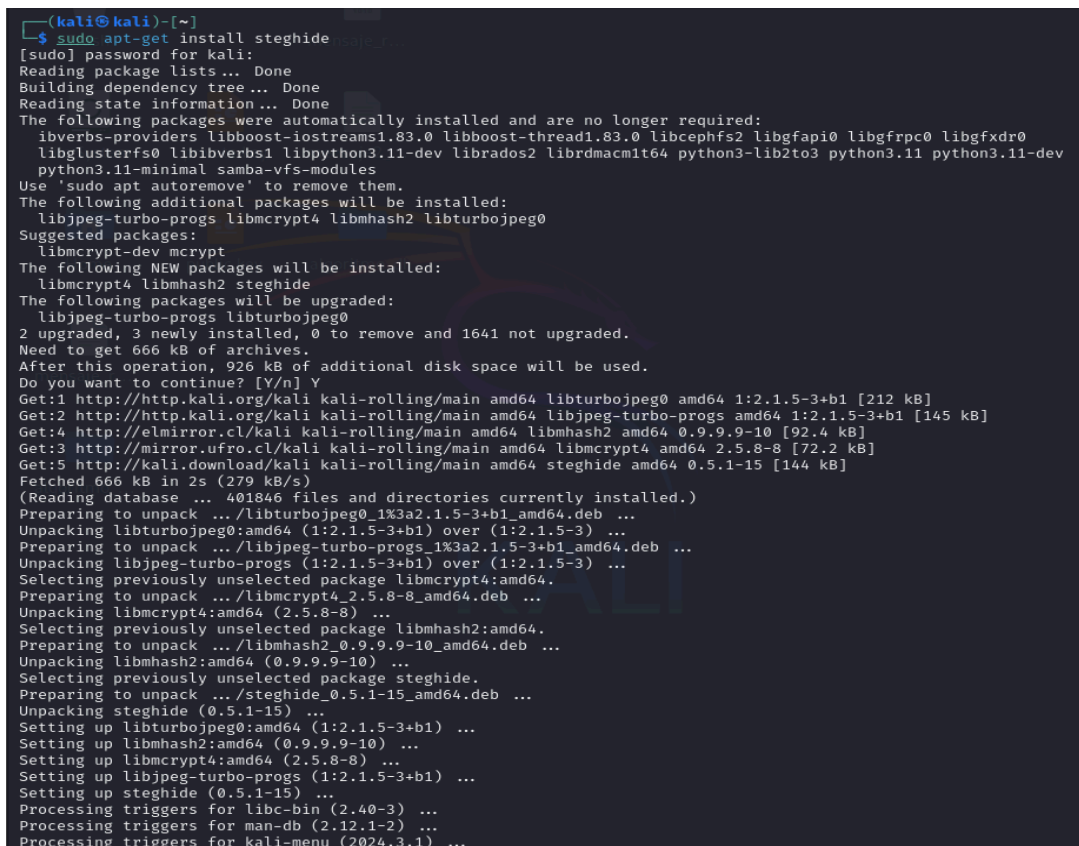
```
(kali@kali)-[~]
$ setxkbmap -layout latam
(kali@kali)-[~]
$
```

3. Se actualiza el repositorio de Kali con el comando `sudo apt-get update`



```
(kali@kali)-[~]
$ sudo apt-get update
[sudo] password for kali:
Get:1 http://elmirror.cl/kali kali-rolling InRelease [41.5 kB]
Get:2 http://elmirror.cl/kali kali-rolling/main i386 Packages [19.8 MB]
Get:3 http://elmirror.cl/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:4 http://elmirror.cl/kali kali-rolling/main i386 Contents (deb) [46.2 MB]
Get:5 http://elmirror.cl/kali kali-rolling/main amd64 Contents (deb) [49.4 MB]
Get:6 http://elmirror.cl/kali kali-rolling/contrib i386 Packages [94.9 kB]
Get:7 http://elmirror.cl/kali kali-rolling/contrib amd64 Packages [112 kB]
Get:8 http://elmirror.cl/kali kali-rolling/contrib amd64 Contents (deb) [274 kB]
Get:9 http://elmirror.cl/kali kali-rolling/contrib i386 Contents (deb) [190 kB]
Get:10 http://elmirror.cl/kali kali-rolling/non-free i386 Packages [150 kB]
Get:11 http://elmirror.cl/kali kali-rolling/non-free amd64 Packages [197 kB]
Get:12 http://elmirror.cl/kali kali-rolling/non-free i386 Contents (deb) [823 kB]
Get:13 http://elmirror.cl/kali kali-rolling/non-free amd64 Contents (deb) [877 kB]
Fetched 139 MB in 27s (5,124 kB/s)
Reading package lists... Done
```

4. Se instala la herramienta Steghide con el comando:
`sudo apt-get install steghide`



```
(kali@kali)-[~]
$ sudo apt-get install steghide
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfs2 libgfrpc0 libgfsxdr0
  libglusterfs0 libibverbs1 libpython3.11-dev librados2 librdmacm164 python3-lib2to3 python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libjpeg-turbo-progs libmbedtls libmhash2 libturbojpeg0
Suggested packages:
  libmbedtls-dev mcrack
The following NEW packages will be installed:
  libmbedtls libmhash2 steghide
The following packages will be upgraded:
  libjpeg-turbo-progs libturbojpeg0
2 upgraded, 3 newly installed, 0 to remove and 1641 not upgraded.
Need to get 666 kB of archives.
After this operation, 926 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libturbojpeg0 amd64 1:2.1.5-3+b1 [212 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libjpeg-turbo-progs amd64 1:2.1.5-3+b1 [145 kB]
Get:3 http://elmirror.cl/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9-10 [92.4 kB]
Get:4 http://mirror.ufro.cl/kali kali-rolling/main amd64 libmbedtls amd64 2.5.8-8 [72.2 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 steghide amd64 0.5.1-15 [144 kB]
Fetched 666 kB in 2s (279 kB/s)
(Reading database ... 401846 files and directories currently installed.)
Preparing to unpack .../libturbojpeg0_1%3a2.1.5-3+b1_amd64.deb ...
Unpacking libturbojpeg0:amd64 (1:2.1.5-3+b1) over (1:2.1.5-3) ...
Preparing to unpack .../libjpeg-turbo-progs_1%3a2.1.5-3+b1_amd64.deb ...
Unpacking libjpeg-turbo-progs (1:2.1.5-3+b1) over (1:2.1.5-3) ...
Selecting previously unselected package libmbedtls:amd64.
Preparing to unpack .../libmbedtls_2.5.8-8_amd64.deb ...
Unpacking libmbedtls:amd64 (2.5.8-8) ...
Selecting previously unselected package libmhash2:amd64.
Preparing to unpack .../libmhash2_0.9.9-10_amd64.deb ...
Unpacking libmhash2:amd64 (0.9.9-10) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libturbojpeg0:amd64 (1:2.1.5-3+b1) ...
Setting up libmhash2:amd64 (0.9.9-10) ...
Setting up libmbedtls:amd64 (2.5.8-8) ...
Setting up libjpeg-turbo-progs (1:2.1.5-3+b1) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...
```

5. Se baja un archivo de una imagen en formato jpg, en este caso se guarda como eao.jpg

```
(kali㉿kali)-[~/Downloads]
$ ls -l
total 224
-rw-rw-r-- 1 kali kali 225618 Nov 20 11:37 eao.jpg
```

6. Se crea un archivo de texto con un mensaje, en este caso se guarda como mensaje.txt

```
File Actions Edit View Help
GNU nano 8.1
Este es un mensaje secreto
para usar con Steghide
```

Se visualizan los archivos con el comando

`ls -l`

```
(kali㉿kali)-[~/Downloads]
$ ls -l
total 228
-rw-rw-r-- 1 kali kali 225618 Nov 20 11:37 eao.jpg
-rw-rw-r-- 1 kali kali      50 Nov 20 11:45 mensaje.txt

(kali㉿kali)-[~/Downloads]
$
```

7. Se oculta el archivo de texto en la imagen con el siguiente comando:
`steghide embed -cf eao.jpg -ef mensaje.txt`
Se ingresa una clave para realizar la acción

```
(kali㉿kali)-[~/Downloads]
$ steghide embed -cf eao.jpg -ef mensaje.txt
Enter passphrase:
Re-Enter passphrase:
embedding "mensaje.txt" in "eao.jpg" ... done

(kali㉿kali)-[~/Downloads]
$
```

8. Se borra el archivo de texto "mensaje.txt" con el comando:
`rm mensaje.txt`

```
(kali㉿kali)-[~/Downloads]
$ rm mensaje.txt

(kali㉿kali)-[~/Downloads]
$ ls -l
total 224
-rw-rw-r-- 1 kali kali 225580 Nov 20 11:47 eao.jpg
```

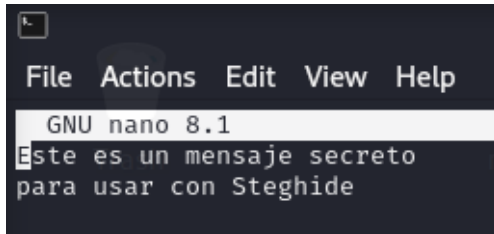
9. Se recupera el mensaje de texto dentro de la imagen eao.jpg con el siguiente comando:

```
steghide extract -sf eao.jpg
```

Se ingresa la clave establecida anteriormente para obtener el mensaje de texto.

```
(kali㉿kali)-[~/Downloads]
$ steghide extract -sf eao.jpg
Enter passphrase:
wrote extracted data to "mensaje.txt".
```

10. Se confirma el contenido en el archivo mensaje.txt

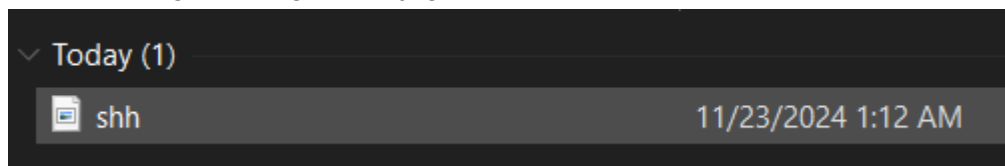


Actividad 4.2: Esteganografía en shh.jpg y ubicación a través de metadatos en 1.jpg

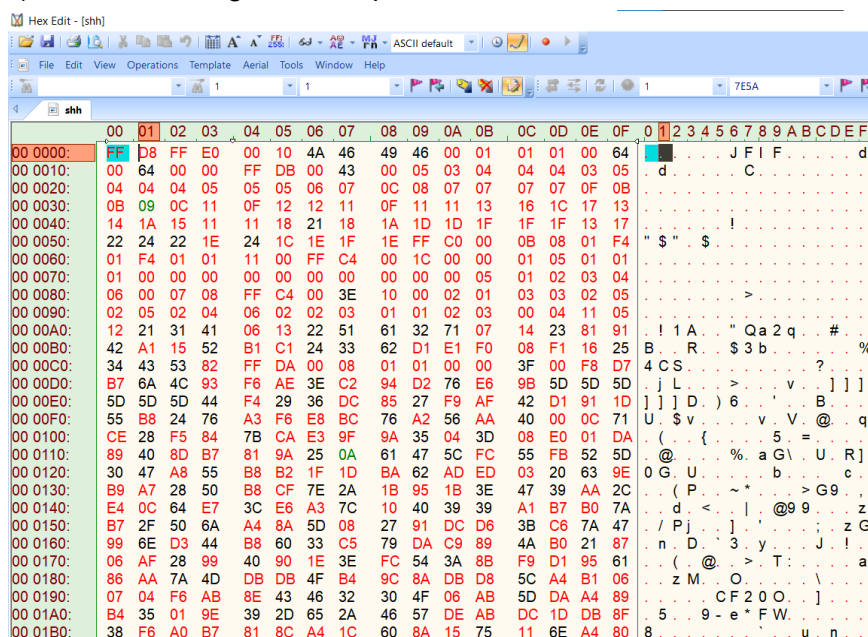
1. Esteganografía en foto shh.jpg

Instrucciones: En la foto shh encontrar a lo menos 10 hallazgos ocultos en la foto (esteganografía)

1) Se descarga la imagen shh.jpg



2) Se abre la imagen en la aplicación Hex Edit



3) En la posición de inicio 9E 41F6 se encuentra FF D8 como inicio de una imagen .jpg

	00	01	02	03	04	05	06	07
9E 41F0:	5E	6C	1A	07	32	6F	FF	D8
9E 4200:	00	01	01	01	00	96	00	96

4) Luego, en la posición final 9E 5612 se encuentra FF D9 como el fin de la imagen

	00	01	02	03
9E 55F0:	A2	8A	28	0
9E 5600:	A2	8A	28	0
9E 5610:	FF	D9		

5) Se copia el rango entre las posiciones y se guarda el archivo como hexed.jpg

85	6E	70	78	04	FB	45	74	4D	F3	3E
F5	DF	73	9E	0B	95	72	DE	F6	D3	FA
8A	CC	D0	28	A2	8A	00	28	A2	8A	00
A2	8A	00	28	A2	8A	00	28	A2	8A	00
07	82	0D	79							D5
82	8B	B3	6F							7A
14	AC	B7	1D							13
6E	3E	16	69							D5
FE	7D	AB	D2							F8
67	4C	95	35							D7
05	86	DD	65							48
6B	D2	68	AA							28
A2	80	31	BC							13
25	C6	91	AB							C9
43	A3	06	5C							C5
15	C9	E0	E7							5E
65	A9	6B	A8							78
DC	8F	99	10							3B
83	75	67	E7							81
5A	CE	9B	A1	E9	F6	1A	AD	D5	B4	36
70	C9	9C	5D	FC	A8	D9	88	C9	F5	D6

File name:

Save as type:

Hide Folders

6) Se abre la aplicación PhotoFiltre y se visualiza la imagen hexed.jpg, la cual contiene un mensaje oculto, la palabra “GL0zMε”



7) Luego, en la posición 7E5A se encuentra el carácter Z en ASCII, representado por 5A que en conjunto a los demás genera la palabra Zar!

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00 7DE0:	F4	26	E6	47	79	06	E3	43	75	2F	4B	8C	56	53	C5	8A	.	&	Gy	.	Cu	/	K	.	V	S	
00 7DF0:	19	0E	79	F4	57	87	FE	20	22	98	5D	C8	E5	70	47	F3	.	y	W	.	"]	.	p	G		
00 7E00:	58	78	27	72	0E	71	C6	6B	A0	76	17	23	18	1D	EA	A6	X	x	'	r	q	.	k	.	v	#		
00 7E10:	A8	A3	CF	63	8E	87	15	45	E4	72	71	9A	8C	B1	CD	26	.	.	c	.	E	.	r	q		
00 7E20:	79	E6	92	BA	BA	9C	2A	49	7E	A0	6A	33	D4	57	2F	7A	y	.	.	.	*	l	~	j	3	.	W	/	z	.		
00 7E30:	E1	D0	D2	0A	50	70	C0	FB	51	7B	79	19	E0	05	B1	CF	.	.	.	P	p	.	Q	{	y		
00 7E40:	C5	5C	BE	45	F2	95	BB	E0	29	F9	06	B3	D2	8D	B2	B2	.	.	\	.	E		
00 7E50:	82	70	0E	2A	C6	D0	40	35	FF	D9	5A	61	72	21	1A	07	.	.	p	.	*	.	@	5	.	.	Z	a	r	!		
00 7E60:	00	CE	99	73	80	00	0D	00	00	00	00	00	00	00	0E	15	.	.	s		
00 7E70:	77	F1	A4	CB	CB	F2	CE	89	5C	E4	96	2D	2E	F5	58	B5	w		
00 7E80:	A3	A5	46	46	1C	6F	C7	B7	FE	52	93	67	64	C2	C3	1C	.	.	F	F	.	o	.	.	.	R	.	g	d	.		
00 7E90:	EA	23	AD	7C	38	E9	27	6C	B7	28	43	E9	52	48	B6	B1	.	.	#	.		8	.	'	l	.	(C	.	R	H	
00 7EA0:	F7	9C	18	8E	22	EA	4A	7B	CD	CA	34	77	1F	09	4B	B8	"	.	J	{	.	4	w	.	.	K	.	
00 7EB0:	68	3B	38	02	89	A3	72	40	66	EE	BF	95	1A	93	BB	54	h	.	;	8	.	.	r	@	T	.	
00 7EC0:	D0	F7	FE	2C	DC	62	99	75	F1	2F	FD	C2	E4	7E	4A	37	b	.	u	.	.	/	.	.	~	J	7	
00 7ED0:	4A	D3	4F	D2	AE	05	F9	DB	5D	B1	02	68	D6	0E	C8	77	J	.	O	h	.	w
00 7EE0:	04	76	41	24	13	2D	05	9C	EF	9E	F1	B9	A8	F6	4F	F8	.	.	v	.	A	.	\$	O	.

8) Se modifica el carácter Z para obtener la cabecera correcta, representada por la palabra en ASCII Rar! (52 61 72 21 en Hexadecimal)

00 7DF0:	19	0E	79	F4	57	87	FE	20	22	98	5D	C8	E5	70	47	F3	.	.	y	W	.	"]	.	p	G	
00 7E00:	58	78	27	72	0E	71	C6	6B	A0	76	17	23	18	1D	EA	A6	X	x	'	r	q	.	k	.	v	#	
00 7E10:	A8	A3	CF	63	8E	87	15	45	E4	72	71	9A	8C	B1	CD	26	.	.	c	.	E	.	r	q	
00 7E20:	79	E6	92	BA	BA	9C	2A	49	7E	A0	6A	33	D4	57	2F	7A	y	.	.	.	*	l	~	j	3	.	W	/	z	.		
00 7E30:	E1	D0	D2	0A	50	70	C0	FB	51	7B	79	19	E0	05	B1	CF	.	.	.	P	p	.	Q	{	y	
00 7E40:	C5	5C	BE	45	F2	95	BB	E0	29	F9	06	B3	D2	8D	B2	B2	.	.	\	.	E	
00 7E50:	82	70	0E	2A	C6	D0	40	35	FF	D9	52	61	72	21	1A	07	.	.	p	.	*	.	@	5	.	.	R	a	r	!	.	
00 7E60:	00	CE	99	73	80	00	0D	00	00	00	00	00	00	00	0E	15	.	.	s
00 7E70:	77	F1	A4	CB	CB	F2	CE	89	5C	E4	96	2D	2E	F5	58	B5	w
00 7E80:	A3	A5	46	46	1C	6F	C7	B7	FE	52	93	67	64	C2	C3	1C	.	.	F	F	.	o	.	.	.	R	.	g	d	.	.	.
00 7E90:	EA	23	AD	7C	38	E9	27	6C	B7	28	43	E9	52	48	B6	B1	.	.	#	.		8	.	'	l	.	(C	.	R	H	.

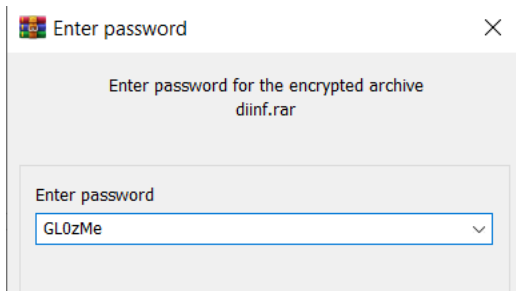
9) Para obtener el archivo .rar se elimina todo el contenido previo a la palabra Rar! realizando un corte de la información anterior.

00	01	02	03	04	05	06	07	08
FF	D8	FF	E0	00	10	4A	46	49
00	64	00	00	FF	DB	00	43	00
04	04	04	05	05	05	06	07	0C
0B	09	0C	11	0F	12	12	11	0F
14	1A	15	11	11	18	21	18	1A
22	24	22						
01	F4	01						
01	00	00						
06	00	07						
02	05	02						
A3	A5	46	46	1C	6F	C7	B7	FE
52	61	72	21	1A	07			

10) Ahora, se guarda el archivo obtenido con extensión .rar, para este caso se usa diinf.rar

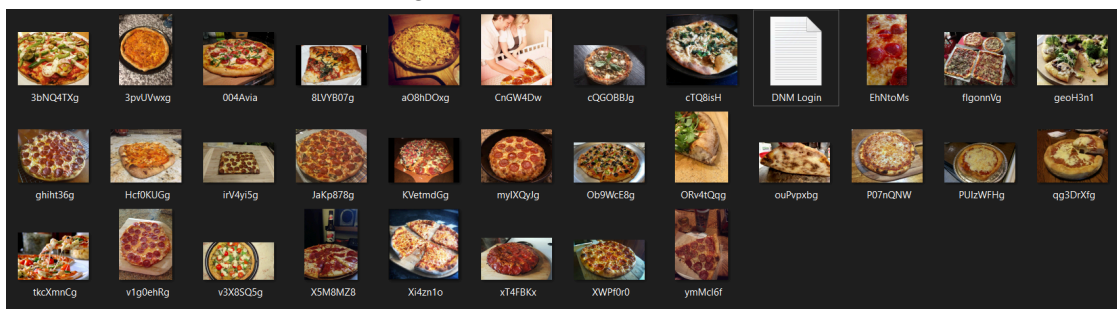
File name:	diinf.rar
Save as type:	All Files (*.*)

11) Se cierra la aplicación Hex Edit y se procede a descomprimir el archivo diinf.rar. Se pide una contraseña por lo que se usará la palabra obtenida anteriormente "GL0zMe" para descomprimir el archivo.



diinf	11/23/2024 1:30 AM	WinRAR archive	10,102 KB
diinf	11/23/2024 1:34 AM	File folder	

12) Al abrir la carpeta se logran obtener los archivos ocultos: 31 imágenes .jpg de pizzas y un archivo .txt llamado DNM Login



DNM Login - Notepad

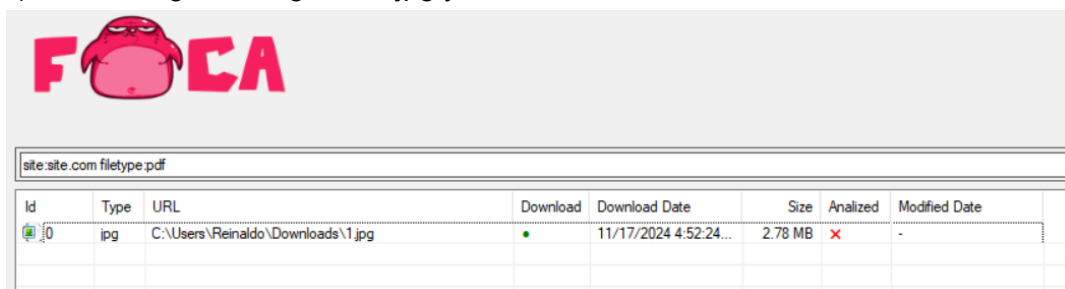
File Edit Format View Help

PapaSmurphye -- HTS{You_caught_me!}

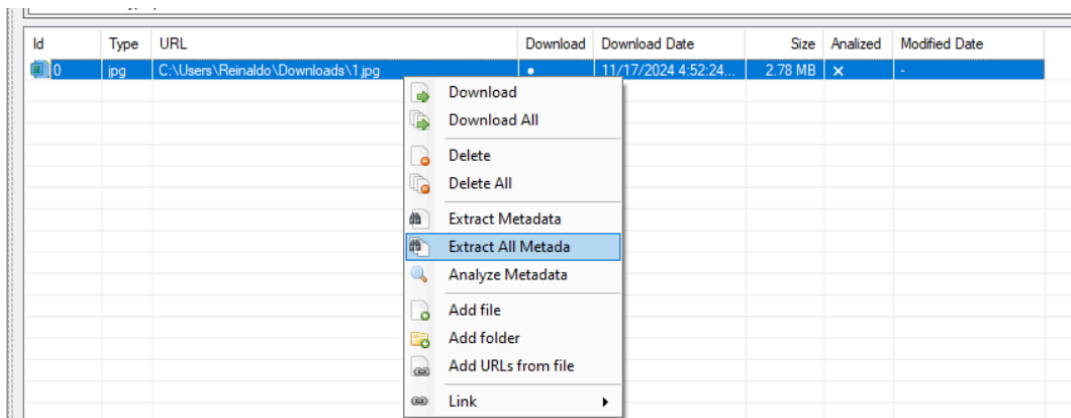
2. Buscar ubicación a través de metadatos en imagen 1.jpg

Instrucciones: Indique toda la información que pueda entregar de la fotografía además de la geolocalización indicando la dirección exacta donde se sacó la fotografía , buscándola en google maps u otro aplicativo , etc.

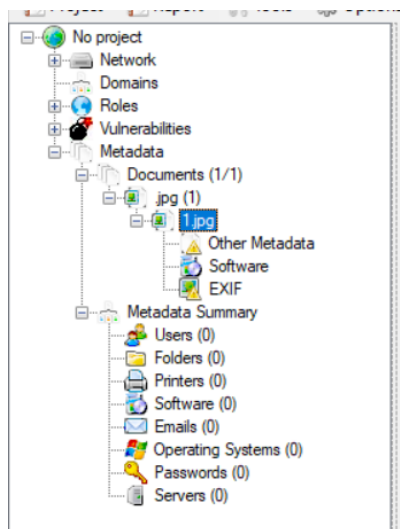
1) Se descarga la fotografía 1.jpg y se arrastra en el software FOCA



2) Se selecciona la fotografía y se presiona en “Extract All Metadata” para obtener todos los metadatos



3) Se visualiza que se obtuvieron los metadatos, para revisarlos, se presiona en EXIF para ver el archivo de metadatos



4) En el archivo EXIF se logran ver datos relevantes:

- El dispositivo con el que se tomó la fotografía fue un Apple iPhone SE de 2da generación.
- Se pueden ver las configuraciones de la cámara y resolución
- El día en que se tomó la fotografía fue el 29 de Octubre del 2021 a las 01:12:12 de la madrugada.

Exif Makernote	
Make	Apple
Model	iPhone SE (2nd generation)
Orientation	Right side, top (Rotate 90 CW)
X Resolution	72 dots per inches
Y Resolution	72 dots per inches
Resolution Unit	Inches
Software	14.7.1
Date/Time	2021:10:29 01:12:12
Tile Width	512
Tile Length	512
YCbCr Positioning	Center of pixel array
Exposure Time	1/15 sec
F-Number	F 1.8
Exposure Program	Program normal
ISO Speed Ratings	800
Exif Version	2.32
Date/Time Original	2021:10:29 01:12:12
Date/Time Digitized	2021:10:29 01:12:12

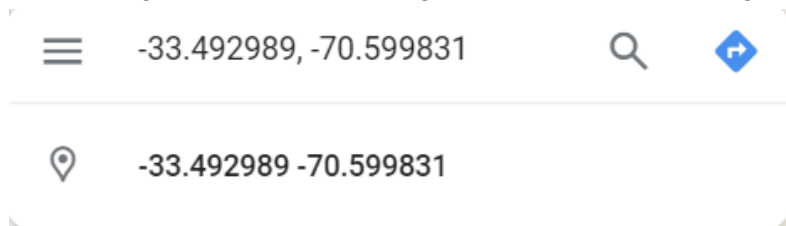
5) En la sección de GPS Exif Makernote se pueden visualizar datos de geolocalización los cuales son relevantes para detectar la ubicación en donde fue tomada la fotografía.

- GPS Latitude Ref: S
- GPS Latitude: 33°29'34.76
- GPS Longitude Ref: W
- GPS Longitude: 70°35'59.39

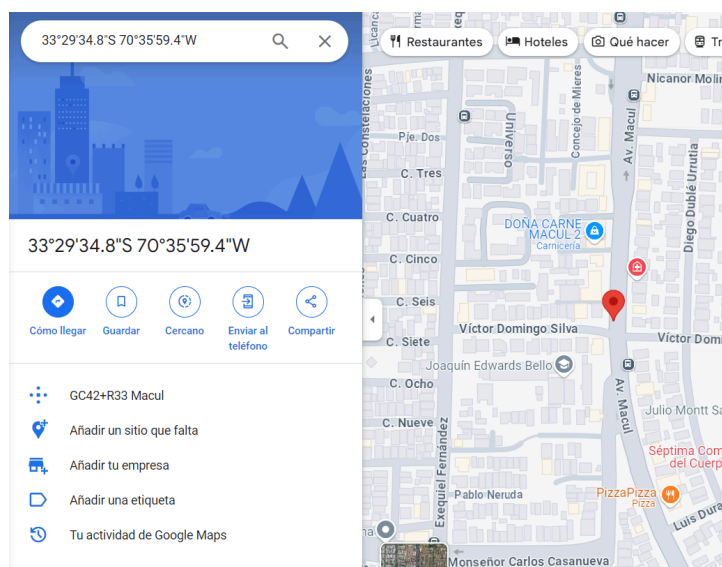
Las coordenadas corresponden a (33°29'34.76"S, 70°35'59.39"W)

GPS Makernote	
GPS Latitude Ref	S
GPS Latitude	33°29'34.76
GPS Longitude Ref	W
GPS Longitude	70°35'59.39
GPS Altitude Ref	Sea level
GPS Altitude	925307/1623 metres
GPS Speed Ref	kph
GPS Speed	9089/154206
GPS Img Direction Ref	True direction
GPS Img Direction	192858/1049 degrees
GPS Dest Bearing Ref	True direction
GPS Dest Bearing	192858/1049 degrees

6) En Google Maps podemos ingresar la información de geolocalización obtenida



7) La ubicación corresponde a la intersección entre la Av. Macul y Víctor Domingo Silva en la comuna de Macul



8) Luego en Google Street View se puede visualizar que la foto fue sacada en el panel de publicidad del paradero PD70-Avenida Macul / Esquina Víctor Diego Silva por lo cual la geolocalización es correcta.



Imagen original



Imagen Google Street View