RETO 3

SEGURIDAD Y ATAQUES INFORMÁTICOS

Pablo Ramiro Foronda

Marianela Estévez Bosso

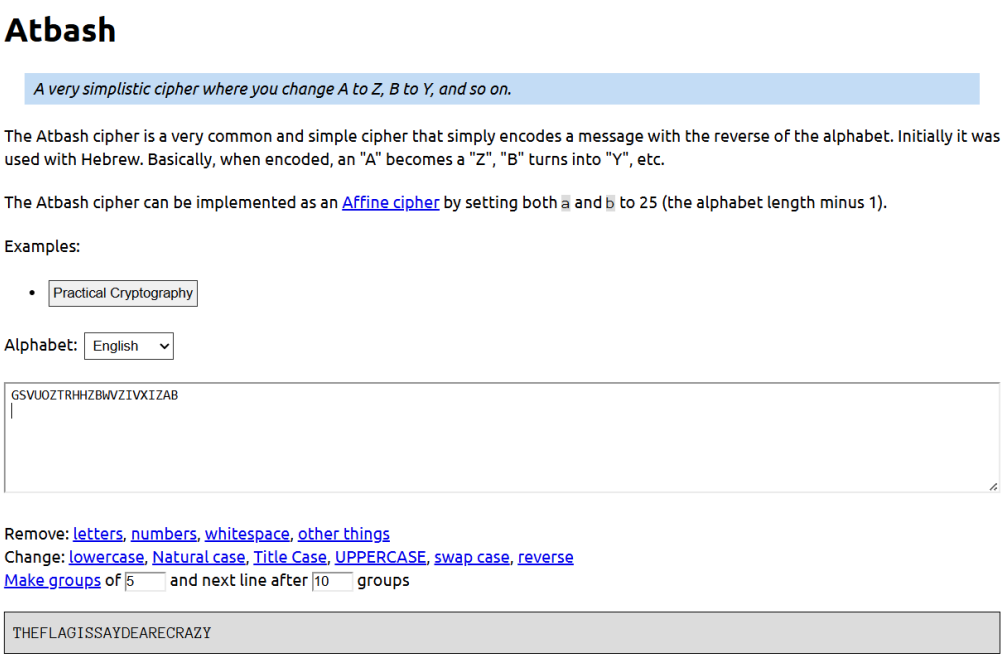
Ignacio García García

Guillermo Rojo Martín

NIVEL INICIACIÓN

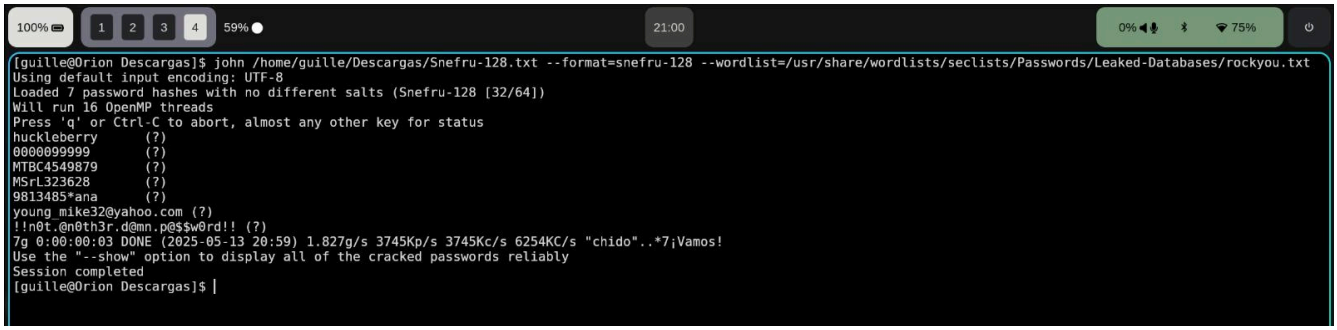
- Magic Crypto

Para descifrar el mensaje oculto en la imagen con el método Atbash: GSVUOZTRHHZBWVZIVXIZAB. Reemplazamos cada letra del alfabeto con su opuesta el mensaje cifrado queda **THE FLAG IS SAY WE ARE CRAZY**



- Hash Cracking

Los hashes en el archivo están generados con el algoritmo Snefru-128. Con el programa John the Ripper y usando el comando con el texto obtenemos:



El único resultado que no contiene números: **huckleberry**.

- Calculator

En este reto, nos proporcionaron imágenes que mostraban un código en Python. El programa pedía introducir un número entre 82 y 93 y, dependiendo del valor, devolvía un mensaje distinto. Analizamos la estructura del código y observamos cómo se concatena cadenas según el número y si era par o impar.

Probando valores dentro del rango e interpretando la lógica, descubrimos que solo introduciendo el número 87 se obtenía la cadena correcta que representa la flag:

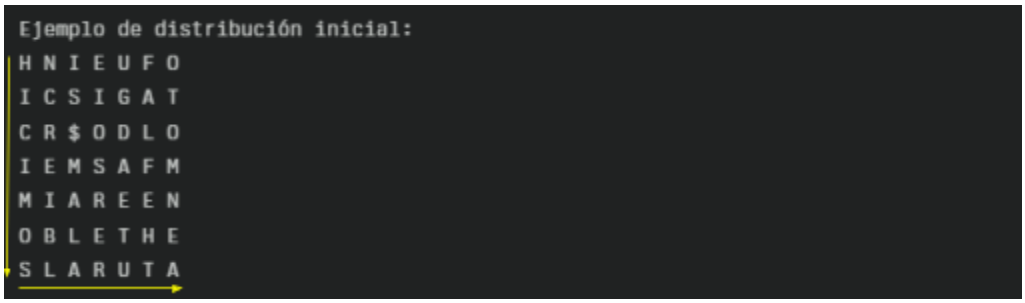
```
$ python calculator.py
Introduce un número: 87
ReAdLe$$tVshHsH
```

Flag obtenido: **ReAdLe$$tVshHsH**

- Ruta

Cadena cifrada: HNIEUFOICSIGATCR$ODLOIEMSAFMMIAREENOBLETHESLARUTA

Es un cifrado por transposición de ruta usando una matriz cuadrada de 7x7 en sentido espiral hacia abajo. Este método reorganiza los caracteres siguiendo patrones geométricos.



- Trazado de la ruta: Sigue la espiral desde la esquina superior izquierda, bajando y yendo en sentido antihorario.

Texto descifrado: **HICIMOSLARUTAENMOTOFUEINCREIBLETHEFLAGIS$MAREADOS**

Flag obtenido: **$MAREADOS**

- El libro del Quijote

El reto consiste en encontrar un mensaje oculto en "el libro más universal de la literatura", es decir, Don Quijote de la Mancha, utilizando un cifrado tipo "Book cipher" con coordenadas dadas en el formato página:línea:palabra.

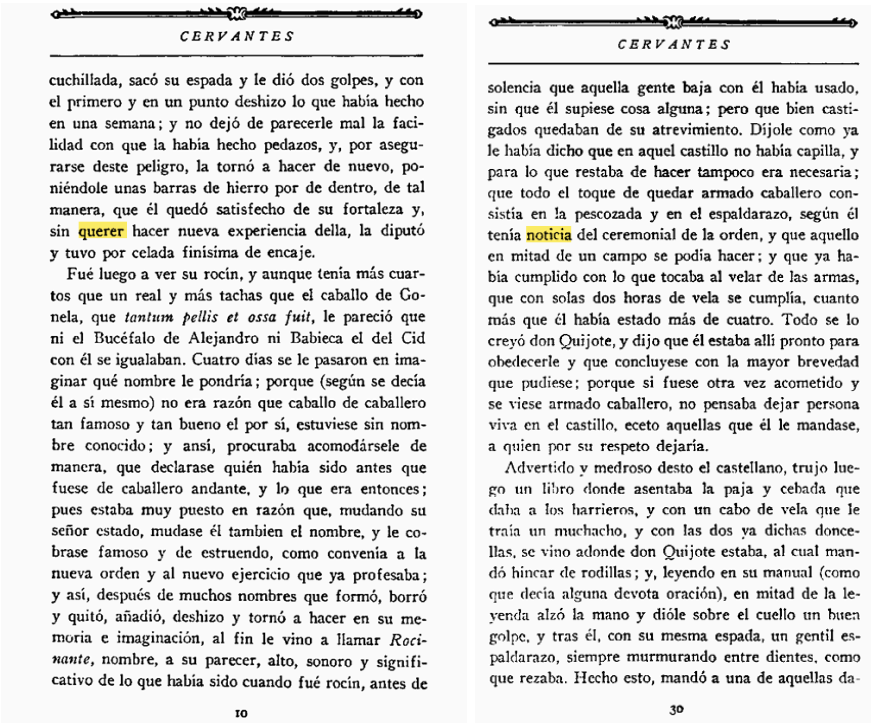
Coordenadas:

- 10:8:2
- 23:10:1
- 30:8:2
- 30:26:7
- 35:1:7
- 151:19:10
- 151:11:8
- 152:11:5

Cada coordenada corresponde a: La página, la línea y la posición de palabra en la línea.

Ejemplo: 10:8:2 indica la palabra número 2 de la línea 8 en la página 10 del PDF proporcionado

Capturas de ejemplo:



CERVANTES

cuchillada, sacó su espada y le dió dos golpes, y con el primero y en un punto deshizo lo que había hecho en una semana; y no dejó de parecerle mal la facilidad con que la había hecho pedazos, y, por asegurarse deste peligro, la tornó a hacer de nuevo, poniéndole unas barras de hierro por de dentro, de tal manera, que él quedó satisfecho de su fortaleza y, sin querer hacer nueva experiencia della, la diputó y tuvo por celada finísima de encaje.

Fué luego a ver su rocín, y aunque tenía más cuartos que un real y más tachas que el caballo de Gonela, que *tantum pellis et ossa fuit*, le pareció que ni el Bucéfalo de Alejandro ni Babieca el del Cid con él se igualaban. Cuatro días se le pasaron en imaginar qué nombre le pondría; porque (según se decía él a sí mesmo) no era razón que caballo de caballero tan famoso y tan bueno el por sí, estuviese sin nombre conocido; y así, procuraba acomodársele de manera, que declarase quién había sido antes que fuese de caballero andante, y lo que era entonces; pues estaba muy puesto en razón que, mudando su señor estado, mudase él tambien el nombre, y le cobrase famoso y de estruendo, como convenía a la nueva orden y al nuevo ejercicio que ya profesaba; y así, después de muchos nombres que formó, borró y quitó, añadió, deshizo y tornó a hacer en su memoria e imaginación, al fin le vino a llamar *Rocinante*, nombre, a su parecer, alto, sonoro y significativo de lo que había sido cuando fué rocín, antes de

10

CERVANTES

solencia que aquella gente baja con él había usado, sin que él supiese cosa alguna; pero que bien castigados quedaban de su atrevimiento. Díjole como ya le había dicho que en aquel castillo no había capilla, y para lo que restaba de hacer tampoco era necesaria; que todo el toque de quedar armado caballero consistía en la pescozada y en el espaldarazo, según él tenía noticia del ceremonial de la orden, y que aquello en mitad de un campo se podía hacer; y que ya había cumplido con lo que tocaba al velar de las armas, que con solas dos horas de vela se cumplía, cuanto más que él había estado más de cuatro. Todo se lo creyó don Quijote, y dijo que él estaba allí pronto para obedecerle y que concluyese con la mayor brevedad que pudiese; porque si fuese otra vez acometido y se viese armado caballero, no pensaba dejar persona viva en el castillo, eceto aquellas que él le mandase, a quien por su respeto dejaría.

Advertido y medroso desto el castellano, trujo luego un libro donde asentaba la paja y cebada que daba a los harrieros, y con un cabo de vela que le traía un muchacho, y con las dos ya dichas doncellas, se vino adonde don Quijote estaba, al cual mandó hincar de rodillas; y, leyendo en su manual (como que decía alguna devota oración), en mitad de la leyenda alzó la mano y dióle sobre el cuello un buen golpe, y tras él, con su mesma espada, un gentil espaldarazo, siempre murmurando entre dientes, como que rezaba. Hecho esto, mandó a una de aquellas da-

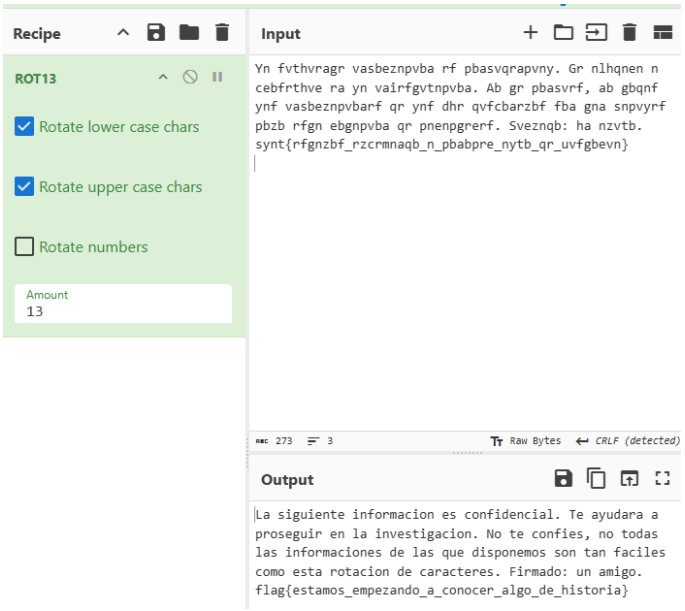
30

Flag final: **querer saber noticias sobre conocer misterio quien hizo**

- Nota Cifrada

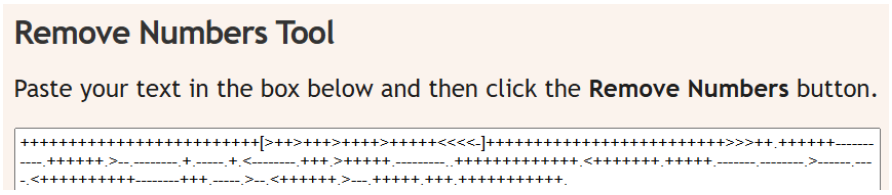
El texto presenta caracteres aparentemente desplazados y las pistas indican un cifrado clásico César, concretamente ROT13 (desplazamiento de 13 posiciones en el alfabeto).

Utilicé la herramienta online CyberChef para aplicar el descifrado ROT13 de manera automática. También comprobé el método manualmente con la flag para demostrar comprensión del proceso. Resultado:



- Warm up level 0

El archivo contiene números intercalados con comandos Brainfuck. Usa expresiones regulares para eliminar todos los dígitos, dejando solo los caracteres válidos de Brainfuck (+, -, >, <, ., ,, [,]). Por lo que hay que hacer una limpieza de código.



++++++++++++++++++++++++++[>++>+++>++++>+++++<<<<-]++++++++++++++++++++++++++>>>++.++++++.----------.++++++.>--.--------.+.-----.+.<--------.+++.>+++++.---------..++++++++++++.<++++++++.+++++.-------.----------.>------.----.<++++.++++++.----.-.---.+++.-----.>--.<++++++.>---.+++++.+++.++++++++++.

Usando un intérprete de Brainfuck nos genera la flag directamente:

flag: **stop bullying sociedad mejor**

- Criptografía lejana

El reto consiste en descifrar un mensaje oculto en una imagen, que contiene el string “NNIGATWAHILHOTCSFE” y la pista “6x3”.

- Se trata de un cifrado de transposición.
- “Cifrado de tipo chino” suele referirse a la lectura por columnas, de derecha a izquierda, en una matriz.
- “6x3” indica las dimensiones de la matriz: 6 columnas y 3 filas.

Se construye la matriz:

N	N	I	G	A	T
W	A	H	I	L	H
O	T	C	S	F	E

Se lee por columnas empezando de derecha a izquierda. La primera columna de arriba a abajo, la segunda de abajo a arriba y así, alternando. Como zigzag.

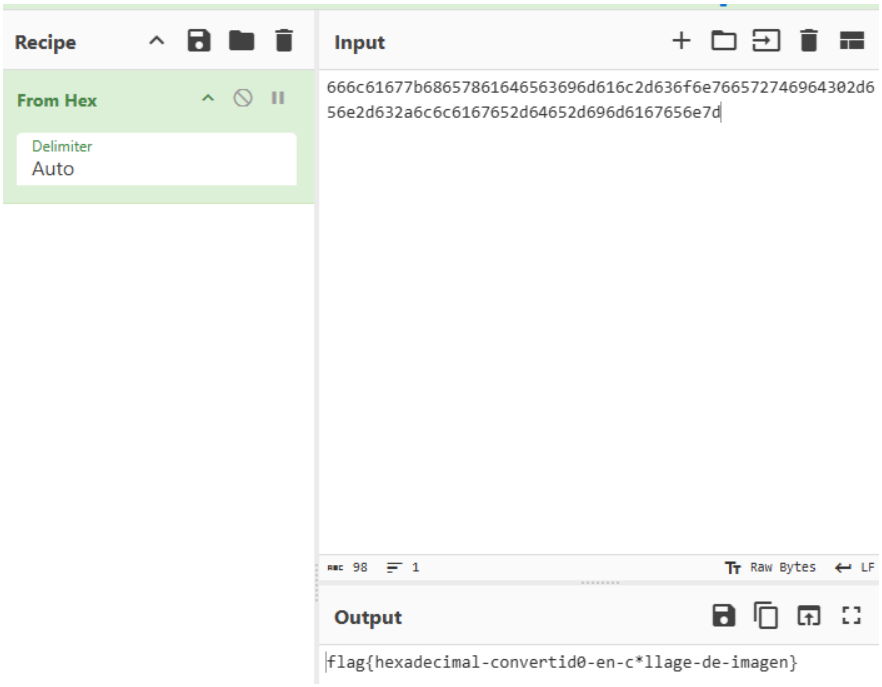
Juntando todo nos queda: **THE FLAG IS CHINATOWN**

NIVEL INTERMEDIO

- Collage

La secuencia de caracteres “flag{}” corresponde exactamente en ASCII a los valores hexadecimales 66 6C 61 67 7B 7D. En el collage se fue relacionando cada imagen con cada carácter hexadecimal, obteniendo la cadena:
666c61677b68657861646563696d616c2d636f6e766572746964302d656e2d632a6c6c6167652d64652d696d6167656e7d

Se usó una herramienta online como CyberChef para convertir la cadena hexadecimal a texto:



flag: **hexadecimal convertid0 en c*llage de imagen**

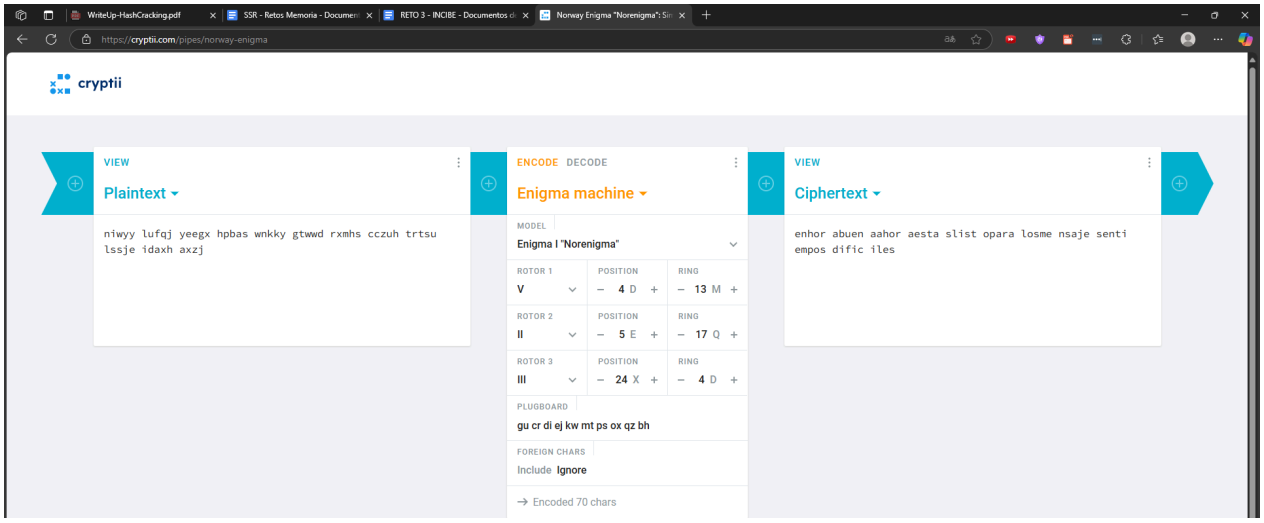
- Rompecabezas

Buscamos las imágenes para ver con que se corresponden, la primera se trata del modelo Enigma 1 y la segunda de Bryggen, Noruega. La suma de las imágenes (1.png + 2.jpg) indica el modelo: Enigma I Norenigma. Usando un traductor, con el resto del texto se deduce que se trata de la configuración inicial de la máquina enigma.

Usamos una página que cifra y descifra con el modelo Norenigma con los parámetros de configuración del fichero.

Solo falta el dato de posición que el fichero dice que corresponde con la extensión de file, file no tiene extensión y no es posible detectar que tipo de fichero es. Al abrirlo se ve que está compilado, lo pasamos a hexadecimal y se ve que la extensión fue borrada. Con strings se pueden encontrar 2 extensiones, dex y jar, además de librerías de android y dalvik. Esto indica que puede ser un archivo dalvik executable o un .jar.

Lo configuramos en la página



Resultado: **enhorabuena ahora estás listo para los mensajes en tiempos difíciles**

NIVEL AVANZADO

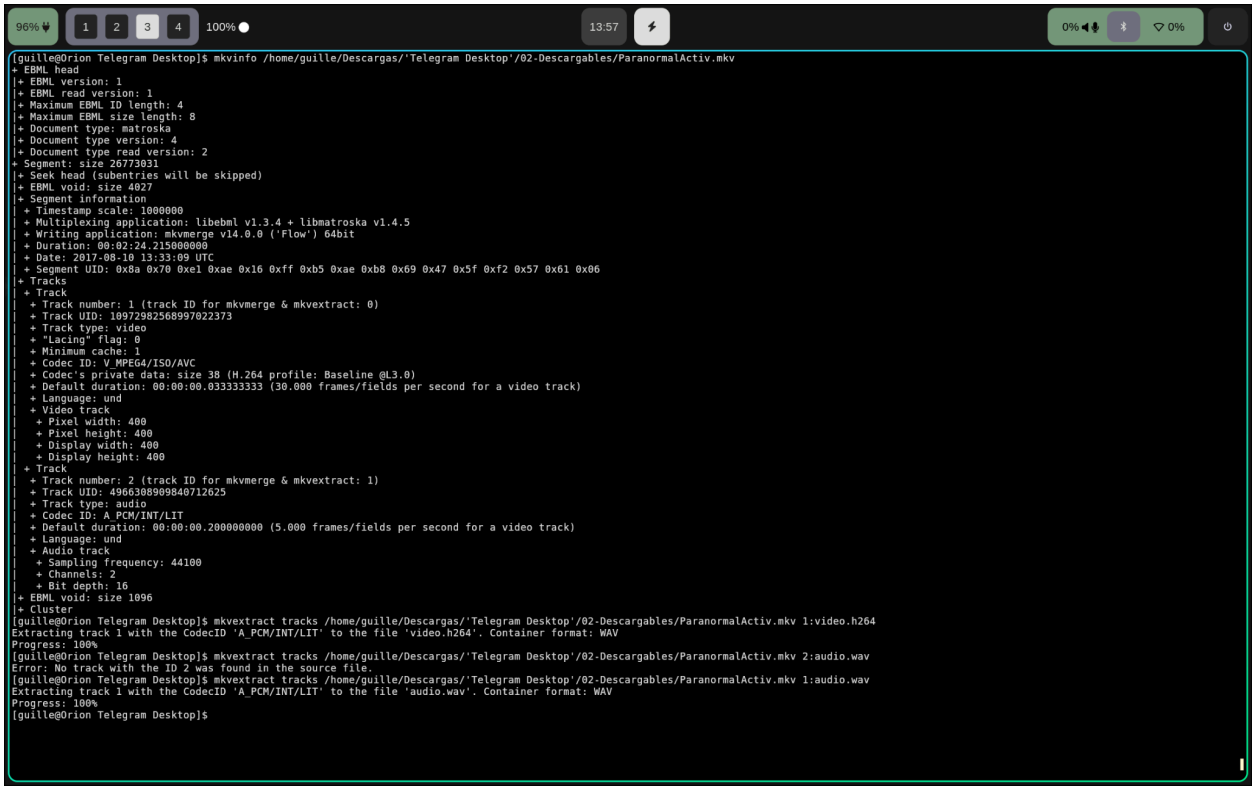
- Paranormal Activity

El archivo .mkv es un contenedor Matroska, capaz de almacenar varias pistas de audio, video y subtítulos.

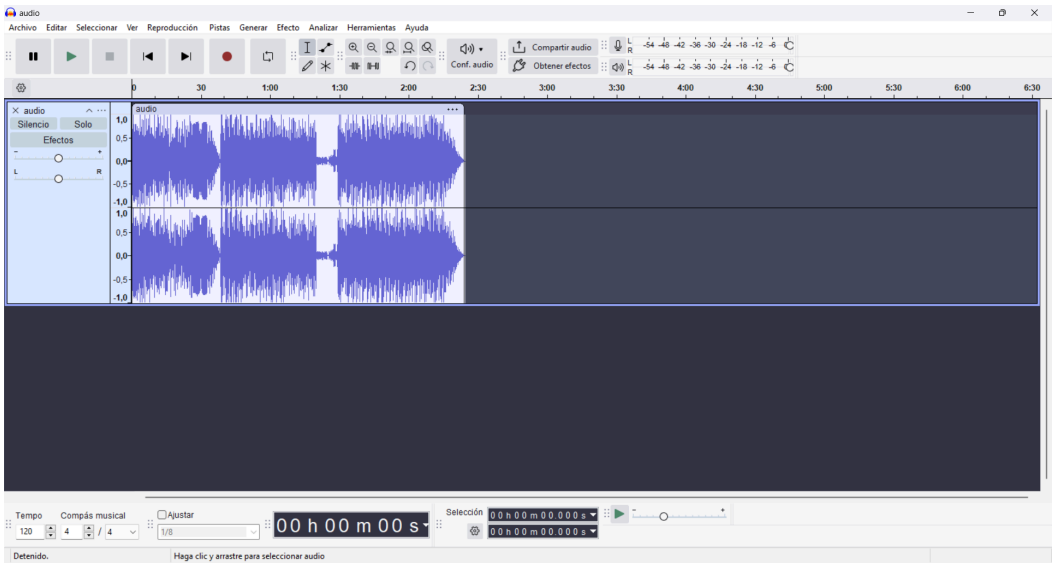
Utilizamos MKVToolNix para extraer las pistas del contenedor.

- Vemos la información del archivo, en el track number 1 podemos ver que está el archivo de video mediante el comando: $ mkvinfo /home/guille/Descargas/'Telegram Desktop'/02-Descargables/ParanormalActiv.mkv.

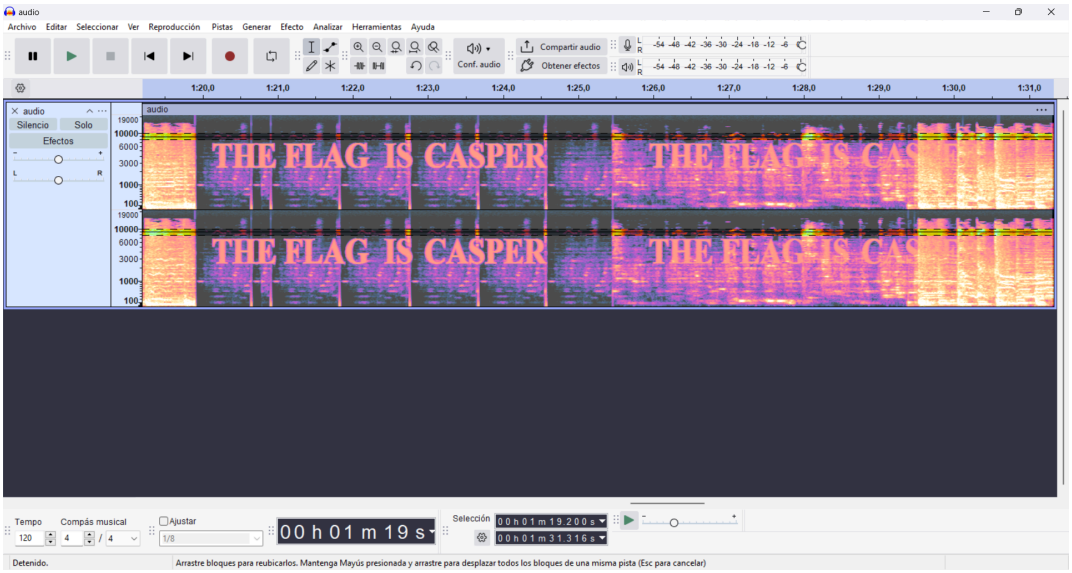
- Del archivo de video extraemos el .h264 y el .wav que es el audio que nos interesa. Finalmente se extrae el audio con el comando: $ mkvextract tracks /home/guille/Descargas/'Telegram Desktop'/02-Descargables/ParanormalActiv.mkv 1:audio.wav



En la aplicación Audacity metemos el audio que extrajimos.



Le damos a Espectrograma, seleccionamos el fragmento donde la amplitud de onda es más pequeña y ampliando la selección. Lo que nos devuelve la flag: **CASPER**



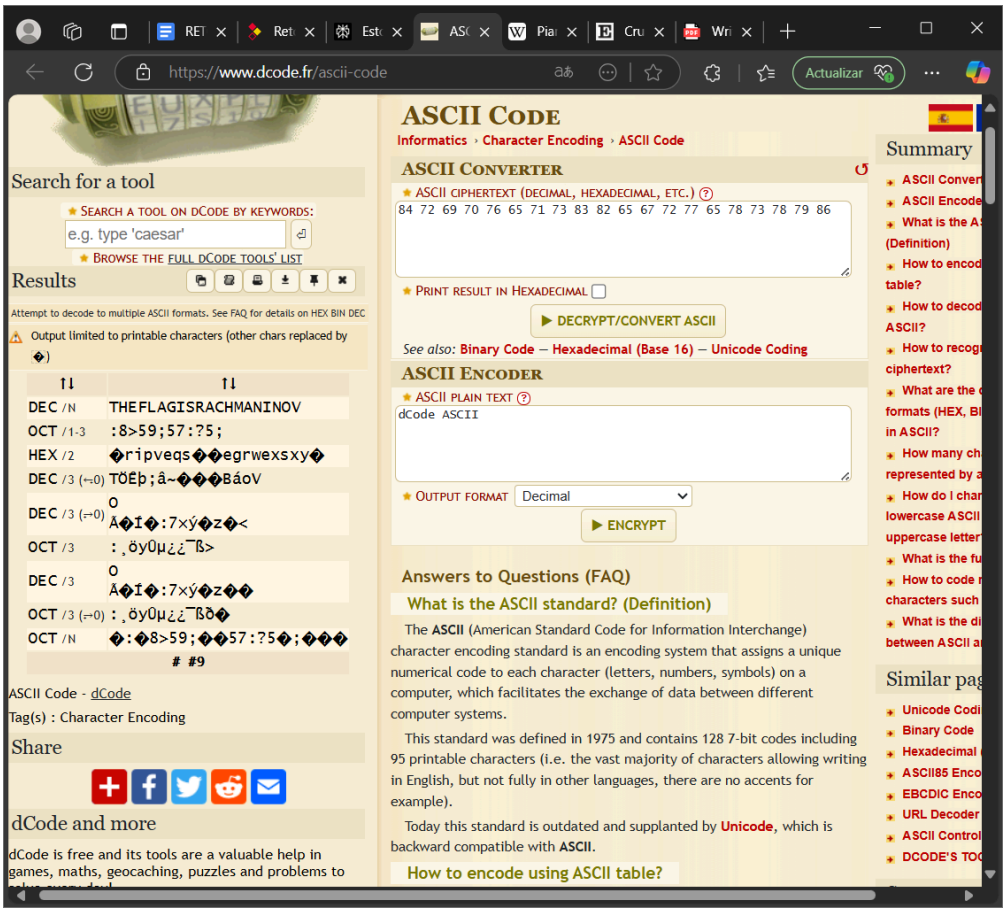
- Suena bien

La partitura muestra una serie de notas musicales, con la firma de Bartolomeo Cristofori (inventor del piano). Al buscar por internet las frecuencias de cada tecla en el piano inglés, obtenemos una imagen con todas estas, incluyendo las 88 teclas de un piano estándar.

Una vez que tenemos la secuencia de teclas, podemos convertirla a texto usando un conversor de código ASCII. En la tabla podemos obtener el número al que se interpreta cada nota de la imagen.

Key number	Helmholtz name	Scientific name	Frequency (Hz)	Corresponding Open Strings				
				Violin	Viola	Cello	Bass	Guitar
88	c⁵ 5-line octave	C8 Eighth octave	4186.01					
87	b⁴	B7	3951.07					
86	a♯⁴/b♭⁴	A♯7/B♭7	3729.31					
85	a⁴	A7	3520.00					
84	g♯⁴/a♭⁴	G♯7/A♭7	3322.44					
83	g⁴	G7	3135.96					
82	f♯⁴/g♭⁴	F♯7/G♭7	2959.96					
81	f⁴	F7	2793.83					
80	e⁴	E7	2637.02					
79	d♯⁴/e♭⁴	D♯7/E♭7	2489.02					
78	d⁴	D7	2349.32					
77	c♯⁴/d♭⁴	C♯7/D♭7	2217.46					
76	c⁴ 4-line octave	C7 Double high C	2093.00					
75	b³	B6	1975.53					
74	a♯³/b♭³	A♯6/B♭6	1864.66					
73	a³	A6	1760.00					
72	g♯³/a♭³	G♯6/A♭6	1661.22					
71	g³	G6	1567.98					
70	f♯³/g♭³	F♯6/G♭6	1479.98					

- Obteniendo así la secuencia: 84 72 69 70 76 65 71 73 83 82 65 67 72 77 65 78 73 78 79 86. Elegimos Decimal y lo convertimos.



Lo que nos devuelve que la flag **RACHMANINOV**