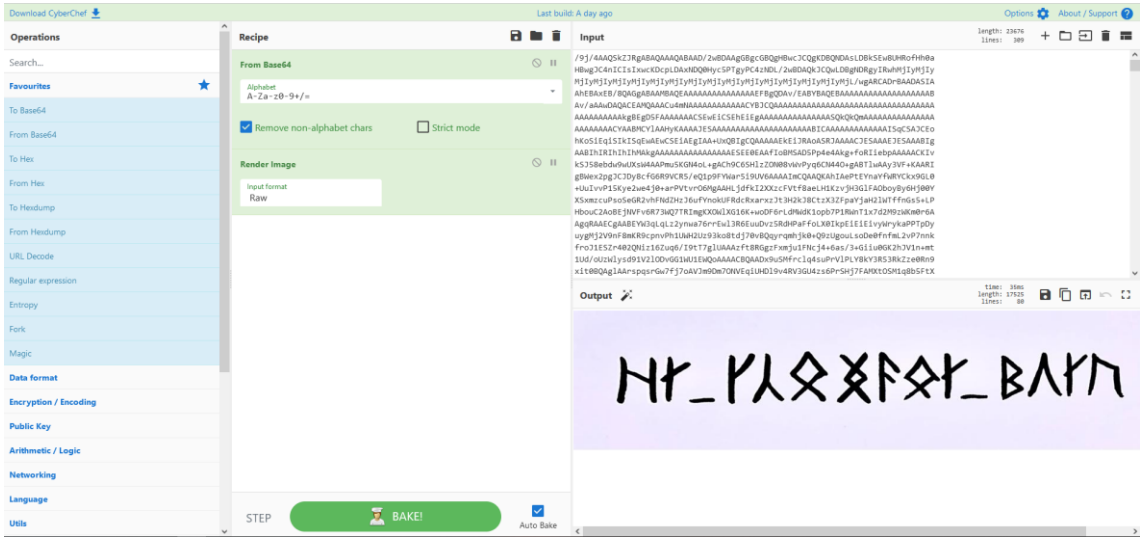
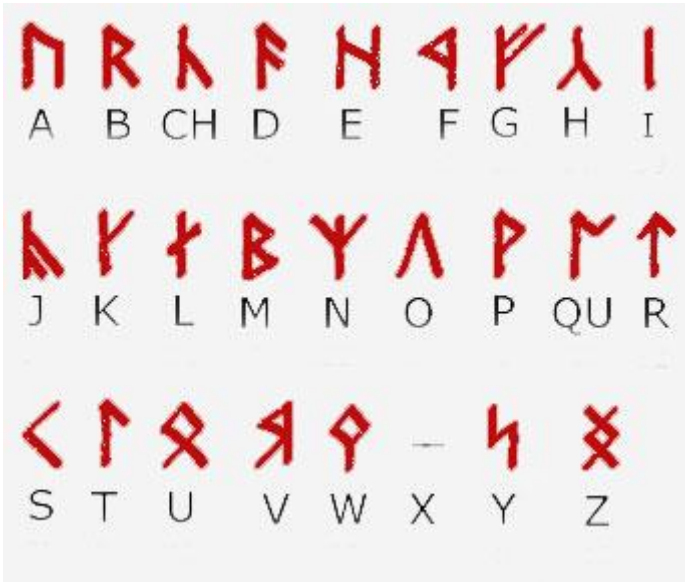
¡Ayuda!-Escaperoom

Auditor: **D3vil2Gh0st**



Pasando el texto **From Base64** y haciendo uso de las herramientas de la página Cyberchef, decodificamos una imagen. Aparentemente los símbolos parecen runas.

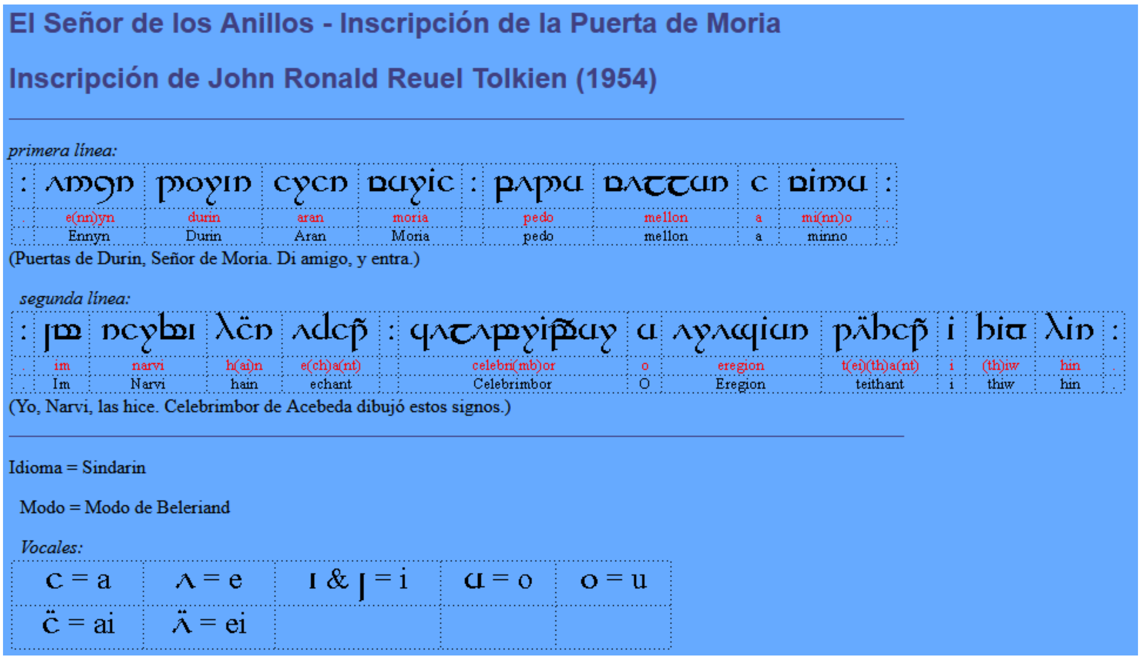
Investigando por internet, parece que el tipo de runas que aparecen son runas de los enanos.



EL_KHUZDUL_MOLA

Trataremos de usar la frase obtenida como contraseña para descomprimir el archivo ZIP. Vemos que no sirve, por lo que tendremos que seguir revisando los archivos obtenidos.

Hay una imagen de la puerta de entrada a las minas de Moria, aunque la inscripción de la puerta está en élfico.



El Señor de los Anillos - Inscripción de la Puerta de Moria

Inscripción de John Ronald Reuel Tolkien (1954)

primera línea:

e(nn)yn	durin	aran	moria	pedo	mellon	a	mi(nn)o
Ennyn	Durin	Aran	Moria	pedo	mellon	a	minno

(Puertas de Durin, Señor de Moria. Di amigo, y entra.)

segunda línea:

im	narvi	h(ai)n	e(ch)a(nt)	celebri(mb)or	o	eregion	t(ei)(th)a(nt)	i	(th)iw	hin
Im	Narvi	hain	echant	Celebrimbor	O	Eregion	teithant	i	thiw	hin

(Yo, Narvi, las hice. Celebrimbor de Acebeda dibujó estos signos.)

Idioma = Sindarin

Modo = Modo de Beleriand

Vocales:

c = a	λ = e	ı & ȷ = i	ɑ = o	o = u
c̈ = ai	λ̈ = ei			

En este caso tenemos la sospecha que la contraseña del archivo ZIP podría coincidir con la palabra que se usaba para abrir las puertas de las minas. Por ahora no creo que recitándola nos ayude a sacar el contenido, así que tiraremos de Parrot para ver que podemos obtener.

```
[D3vil2Gh0st-PC]-[12:44-05/06]-[/home/d3vil2gh0st]
└─d3vil2gh0st$zip2john ./Desktop/key.zip > secret.hash
ver 2.0 efh 5455 efh 7875 key.zip/anPnNYgJ.txt PKZIP Encr: 2b chk, TS_chk, cmplen=300, decmplen=440, crc=1601DE50
ver 2.0 efh 5455 efh 7875 key.zip/B34KLLIW.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=12167, decmplen=12766, crc=9D756954
ver 2.0 efh 5455 efh 7875 key.zip/GAgZpms6.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=12603, decmplen=12801, crc=1E07EBF2
ver 2.0 efh 5455 efh 7875 key.zip/tN6T6QNU.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=17148, decmplen=17370, crc=C33070BD
ver 2.0 efh 5455 efh 7875 key.zip/YuoLN1GR.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=11623, decmplen=11884, crc=8C58100F
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
[D3vil2Gh0st-PC]-[12:44-05/06]-[/home/d3vil2gh0st]
└─d3vil2gh0st$cat secret.hash
key.zip:$pkzip2$3*2*1*0*8*24*9d75*9a2f*ef83ca457b2ac1f4a8ebd47465b2a5ba9e7bf16ac65a1f29f37a1270ae333ef9591677ab*1*0*8*24*1e07*9a33*86160084553d58c02f1ffc82f
4bd557c46d91c282d90cc3b4dd759ef3a0f11ab005651d4*2*0*12c*1b8*1601de50*0*46*8*12c*1601*9b06*fdb03bab1503a4acf391db83c53bc92bdaefc5c2c913966b54c5642c7b39986c6b
5b8b77049f08331d6cdbd781a7064be864d842d175f4e50ce4da5c2a9b73fb8a6d96d344c60b42d9ce0c64ee039c1e30ac8acdb6d096c8f323e324e6751b9713a50556867b738b1b23a49a591608
55353760e7d45f282f0f0bf0d3f174adbdf4732bd93aa4cd3332aa9136b31e2621b39478e18eb881a1a40fe85b30ba1f2976ab76356396c70431d163ecad15d65f23a028d46ebd3ecd942ef59d97
747d15dfdc3bedd734a9ec9206afe7a0a5fd77872c0db0da0009a6637f5e4a9f87f422e3f1a4f7fa73d97b7a99f1974b7efab1b3ca3c5a21d9608624949f04d00b6a2f006d2faf6ad85258443cde
25b35b0cda440b66baf21634046bb92b427e9d9588f578a05354a3547851a12e4a*$/pkzip2$::key.zip:anPnNYgJ.txt, B34KLLIW.jpg, GAgZpms6.jpg:./Desktop/key.zip
[D3vil2Gh0st-PC]-[12:44-05/06]-[/home/d3vil2gh0st]
└─d3vil2gh0st$
```

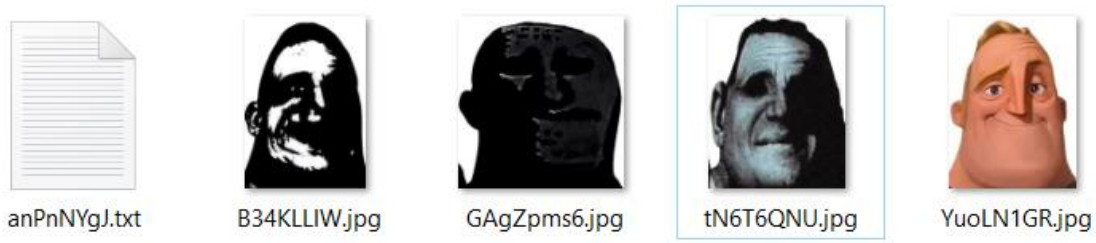
Usando el comando zip2john extraemos el hash que contiene el archivo key.zip, para que nos resulte más sencillo, lo exportaremos a un archivo nombre.hash.

Si hacemos un **cat** del archivo, vemos el hash en formato **PKZIP**. Así que ahora, toca tirar de la herramienta **John the Ripper** para tratar de descifrar la contraseña mediante el hash obtenido.

```
sudo su - Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
┌─[root@D3vil2Gh0st-PC]-[/home/d3vil2gh0st/Desktop]
└──╼ #john --wordlist=/usr/share/wordlists/rockyou2.txt ArchivoKey.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
mellon           (key.zip)
1g 0:00:00:00 DONE (2022-06-05 16:31) 25.00g/s 204800p/s 204800c/s 204800C/s 123456..00112233
Use the "--show" option to display all of the cracked passwords reliably
Session completed
┌─[root@D3vil2Gh0st-PC]-[/home/d3vil2gh0st/Desktop]
└──╼ #
```

Finalmente obtenemos la ansiada contraseña y podemos ver que coincide con la palabra que se recitaba para la apertura de la puerta. **mellon**

Procedemos a extraer el contenido del archivo y obtenemos lo siguiente:



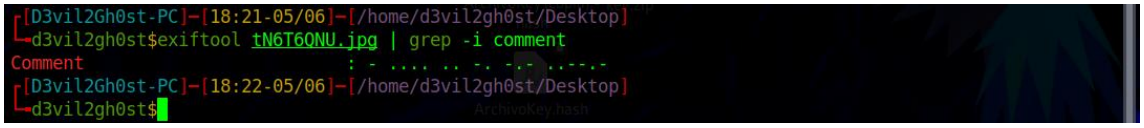
En el archivo de texto vemos lo siguiente:

```
anPnNYgJ.txt: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
0 Notas Investigación- Día 61
1
1 No eran imaginaciones mías, me han robado el anillo y todos mis estudios sobre él. Justo cuando había descubierto el significado del mensaje.
1 No tuve tiempo de recuperarme y tampoco conseguí proteger el anillo.
1 Lo único que puedo hacer ahora es rezar para que alguien, algún día, encuentre esto.
1 Ocultaré mis notas como pueda, trata de reconstruir la clave si consigues verla.
0 Mucha suerte.
1
```

En el texto se comenta que hay notas guardadas que podrían llevar a la clave. Al tener imágenes, podría tratarse de esteganografía o de algún dato que pueda contener la imagen (Metadatos, GPS, Comentarios, etc), así que trataremos de analizar las imágenes.

Haciendo uso de la **Web: https://www.verexif.com** veremos si las imágenes contienen algún dato Exif.

Haciendo uso de la herramienta **exiftool** + **imagen.jpg** y grepeando el contenido de **Comment** obtenemos los mismos valores.




```
┌[D3vil2Gh0st-PC]-[18:22-05/06]-[/home/d3vil2gh0st/Desktop]
└─d3vil2gh0st$exiftool YuoLN1GR.jpg | grep -i comment
Comment                         : -. ..- .-- .
┌[D3vil2Gh0st-PC]-[18:23-05/06]-[/home/d3vil2gh0st/Desktop]
└─d3vil2gh0st$
```

Imagen	Valor Exif Obtenido
GAgZpms6.jpg	Comentario: -.- . -.--
B34KLLIW.jpg	Comentario: .. ..--.-
tN6T6QNU.jpg	Comentario: - .... .. -. -.- ..--.-
YuoLN1GR.jpg	Comentario: -. ..- .-- .

Vemos que en todas las imágenes hay un campo Comentario con un valor que parece Morse.

Usando un traductor de Morse a Texto obtenemos lo siguiente: **KEY IS_ THINK_ NUWE**

Flag{KEYIS_THINK_NUWE}