Misión:

Nivel: Fácil

Introducción:

La flag escondida en esta prueba te va a dar a escoger entre dos opciones. Esperemos que escojas bien, sino vas a recibir las consecuencias...

Información adicional:

URL conseguida: goo.gl/YUNxSu

José Ignacio de Miguel González.

Primero accedemos a esa URL que nos facilitan, y aparece una imagen (bill2.jpg). Aunque Windows si es capaz de abrirla, al intentar abrirla con GIMP nos da un error de que hay caracteres erróneos tras la cadena 0x0A.

La abrimos con un editor hexadecimal, y efectivamente vemos que no termina por la cadena FF D9 por la que terminan las imágenes JPG:

```
0000e5e0h: 36 22 22 6C 43 44 50 43 41 70 0A 43 40 D8 86 88 ; 6""lCDPCAp.C@Ø†ˆ
0000e5f0h: E0 80 57 04 51 FF 0A 61 61 38 31 61 33 30 34 65 ; à€W.Qÿ.aa81a304e
0000e600h: 61 32 61 32 35 61 64 32 39 34 37 61 30 33 30 36 ; a2a25ad2947a0306
0000e610h: 32 63 30 35 66 64 66 D9                         ; 2c05fdfÙ
```

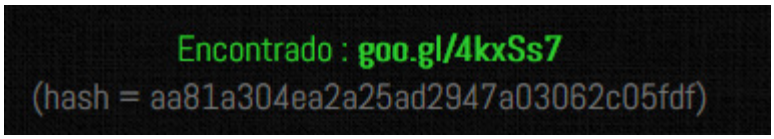
Entre el FF D9 hay un texto en ASCII, probamos a eliminarlo del fichero, dejándolo únicamente con el FF D9 y el fichero ya se abre correctamente en GIMP:

```
0000e5d0h: ED 08 3B 02 8A 80 07 62 02 6C 40 1D A8 09 B5 01 ; í.;.Š€.b.l@.¨.µ.
0000e5e0h: 36 22 22 6C 43 44 50 43 41 70 0A 43 40 D8 86 88 ; 6""lCDPCAp.C@Ø†ˆ
0000e5f0h: E0 80 57 04 51 FF D9                            ; à€W.QÿÙ
```

Por tanto, vamos a analizar ese texto que hemos sacado del fichero:

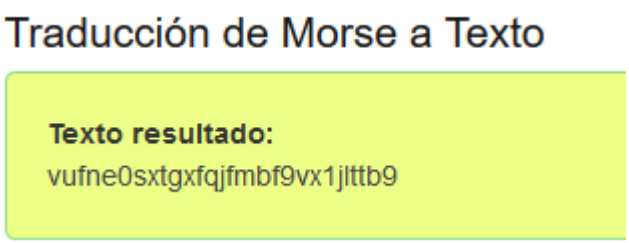
- aa81a304ea2a25ad2947a03062c05fdf

Tiene 32 caracteres, luego puede ser un MD5. SI buscamos esa cadena en https://www.md5online.es/, nos la resuelve así:

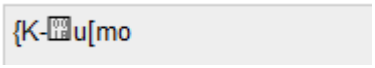


Por tanto, ya tenemos una URL que descargar. De esta URL nos descarga una nueva imagen, si la abrimos con GIMP y jugamos con el contraste y brillo nos aparece lo que parece una cadena morse abajo del todo:

Vamos escribiendo los puntos y rayas en una Web que nos traduce a Morse, y la cadena resultante es:

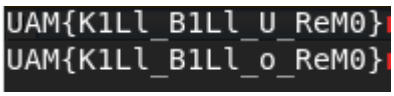


Parece base64, aunque solo en minúsculas es sospechoso, y la decodificación no me da ninguna cadena correcta.



Si la paso a mayúsculas, me empieza a dar un formato parecido al que buscamos, empieza por UAM y termina por "}".

Ahora empiezo a combinar mayúsculas y minúsculas buscando una cadena con sentido, finalmente me salen dos:



En este caso, me voy a inclinar finalmente por la segunda, porque la U no tiene sentido, así que la flag sería UAM{K1Ll_B1Ll_o_ReM0}