RESOLUCIÓN DE EJERCICIOS CRIPTOGRAFIA - UNIDAD 1 SPRINT DOS

INSTRUCCIONES:

Antes de comenzar el ejercicio, crea un directorio llamado <*EjercicioCrypto*>. Dentro del fichero crea un nuevo fichero llamado <*ejercicio_crypto.txt*> y le incorporaras el siguiente texto:

b2pvIGltcG9ydGFudGUgcXVlIGNvZGlmaWNhciBubyBlcyBsbyBtaXN
tbyBxdWUgY2lmcmFy

Para entregar el ejercicio realiza un informe con las capturas de pantalla necesarias para mostrar la ejecución de los ejercicios, mostrando cada enunciado con su imagen correspondiente En esta actividad tendrás que usar tu Kali.

DESCRIPCIÓN Y RESOLUCIÓN:

-- EJERCICIO 1 – FUNCIONES HASH:

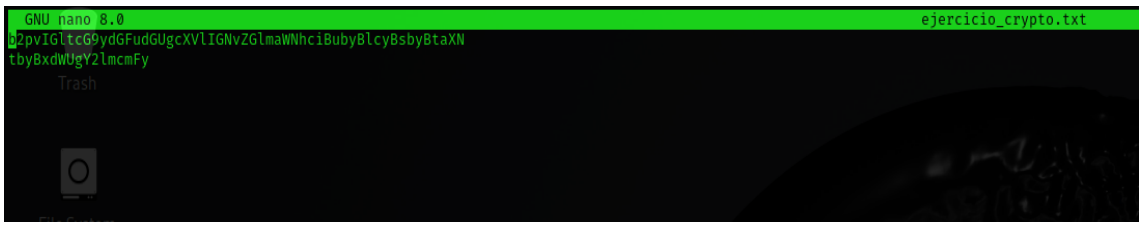
- PREVIO:

- Creo el archivo <ejercicio_crypto> dentro del directorio <EjercicioCrypto>:

```
nano ejercicios_crypto.txt
```

```
❯ cd SPRINT_2
❯ ls
 UNIDAD_1
❯ cd UNIDAD_1
❯ ls
 ejercicio_crypto.txt  hash1.txt  hash2.txt  hash3.txt  hash4.txt
```

- Abro el archivo con nano y le copio el texto.

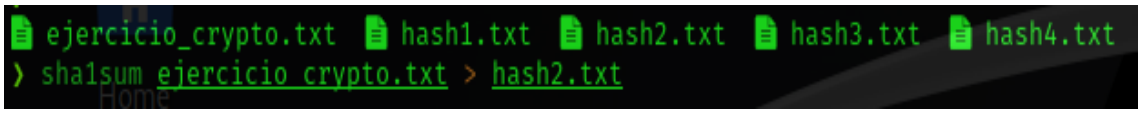


1.- Crea un hash MD5 del fichero ejercicio_crypto.txt y guárdalo como hash1.txt

```
❯ md5sum ejercicio_crypto.txt > hash1.txt
```

```
  GNU nano 8.0                                    hash1.txt
3244441dda3489d1fa5cdb1cf72342dd  ejercicio_crypto.txt
```

2.- Crea un hash SHA-1 del fichero *ejercicio_crypto.txt* y guárdalo como *hash2.txt.*



3.- Crea un hash SHA-256 del fichero *ejercicio_crypto.txt* y guárdalo como *hash3.txt*.

4.- Crea un hash SHA-512 del fichero *ejercicio_crypto.txt* y guárdalo como h*ash4.tx.*

5.- Comprueba con la función “hash-identifier” el resultado de cada uno de los ficheros hash obtenidos anteriormente. ¿Acierta en la predicción del tipo de hash?

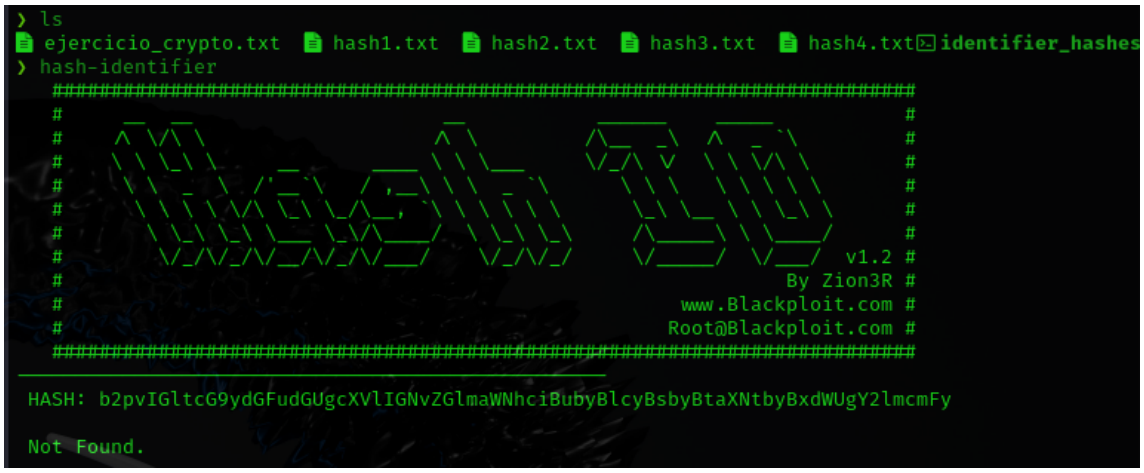
- Realizo un script para que automatice la solución, pero no me funciona con la función hash – identifier pero si con hashid:

```
#!/bin/bash

# Directorio donde se encuentran los archivos de texto
DIR_HASHES="/home/vicevil/BOOT_CIBER_2024/SPRINT_2/UNIDAD_1"

# Iterar sobre cada archivo de texto en el directorio
for archivo in "$DIR_HASHES"/*.txt; do
  echo "Procesando archivo: $archivo"
  # Leer cada línea del archivo y pasarla a hashid
  while read -r linea; do
    # Extraer solo el hash de cada línea y descartar el texto final
    hash=$(echo "$linea" | awk '{print $1}')
    echo "Identificando hash: $hash"
    # Llamar a hashid con el hash
    hashid "$hash"
  done < "$archivo"
done
```

Dando como resultado con el script:

No obstante, como el ejercicio solicita hacerlo con hash – identifier, procedo a realizarlo de forma manual:

1.-



2.-

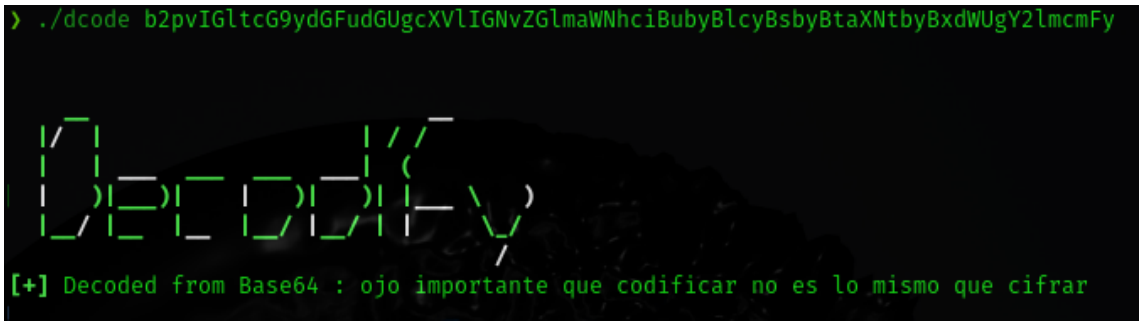
3.-

4.-

5.-

-- EJERCICIO 2 – CODIFICACIÓN:

1.- Decodifica la cadena de texto del fichero *ejercicio_crypto.txt*. ¿En qué codificación se encontraba? En base64.



2. Codifica en el mismo formato la cadena de texto “No metemos gente en criptas”.

Esto se puede directamente en Bash con el comando base64(codificar y decodificar):

o hacerlo a través de la web: https://www.base64encode.org/: