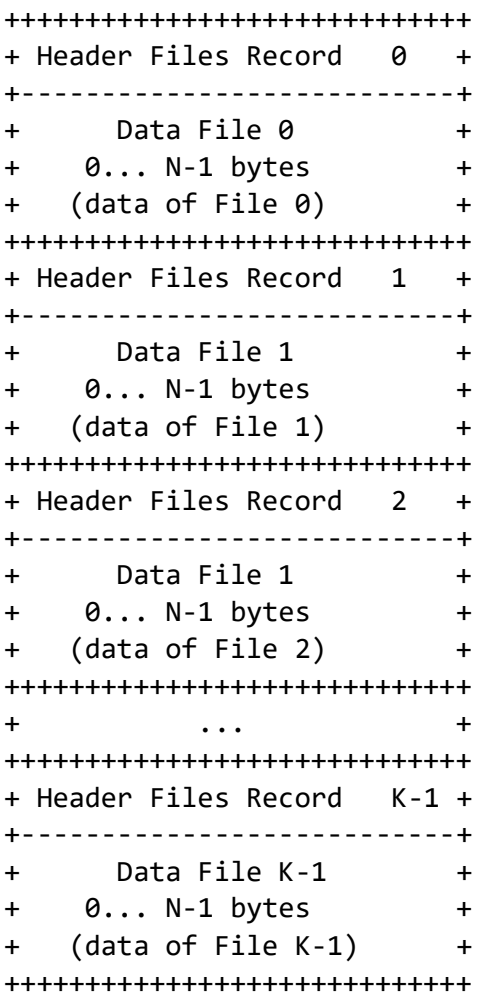
mysha256_repo(ISO)   mysha256_repo specification

NOMBRE
     mysha256_repo - crea un fichero con firmas sha256 de un conjunto de ficheros

UTILIZACION
   ./mysha256_repo uilidad-insertar/utilidad-extraer fich_origen fichero_destino

DESCRIPCION
     mysha256_repo debe crear en fichero_destino un repositorio
     con las propiedades de fich_origen, la firma sha256 del fichero
     y una copia de los datos contenidos.
     El formato del fich_destino del repositorio es el indicado en
     la siguiente figura:
       (1) Source OpenSSL Cryptography and SSL/TLS Toolkit
     https://www.openssl.org/docs/manmaster/man3/SHA256_Init.html
     SHA256_CTX are Deprecated functions. (new EVP_Digest)

     "SPECIAL FILE" Format



```
/**
* @file s_my_sha256header.h
* @author   Gonzalo Alvarez - Dpto. ATC/KAT - UPV-EHU
* @date     05/02/2024
* @brief    Include file with struct c_header_sha256
* @details  A header file(.h) with the data structure definition
*           (c_header_sha256). This file will be used to create a
*           "special file" that will store sha256 hash codes of a
*           set of files.
*
*               "SPECIAL  FILE"
*           ++++++++++++++++++++++++++++
*           + Header Files Record   0   +
*           +--------------------------+
*           +      Data File 0         +
*           +    0... N-1 bytes        +
*           +   (data of File 0)       +
*           ++++++++++++++++++++++++++++
*           + Header Files Record   1   +
*           +--------------------------+
*           +      Data File 1         +
*           +    0... N-1 bytes        +
*           +   (data of File 1)       +
*           ++++++++++++++++++++++++++++
*           + Header Files Record   2   +
*           +--------------------------+
*           +      Data File 1         +
*           +    0... N-1 bytes        +
*           +   (data of File 2)       +
*           ++++++++++++++++++++++++++++
*           +           ...            +
*           ++++++++++++++++++++++++++++
*           + Header Files Record   K-1 +
*           +--------------------------+
*           +      Data File K-1       +
*           +    0... N-1 bytes        +
*           +   (data of File K-1)     +
*           ++++++++++++++++++++++++++++
*
*/
#include <stdlib.h>
#include <stdio.h>
#include <openssl/sha.h>
#include <stddef.h>
#include <errno.h>
#include <string.h>

#define OK (0)
#define ERROR_WRONG_NUMBER_ARGUMENTS (1)
#define ERROR_OPEN_DAT_FILE          (2)
```

```
#define ERROR_READ_DAT_FILE          (3)
#define ERROR_OPEN_SHA_REPO_FILE     (4)
#define ERROR_OTHER_1                (5)
#define ERROR_OTHER_2                (6)

#define FILE_HEADER_SIZE     512
#define READ_BLOCK_SIZE     (16 * 1024)                    // 16 KBytes

// Return error Codes
#define HEADER_OK (1)
#define HEADER_ERR (2)

#define HEX_SHA256_HASH_SIZE  (SHA256_DIGEST_LENGTH*2 +1 )  // 65 Bytes


// Source OpenSSL Cryptography and SSL/TLS Toolkit
//  https://www.openssl.org/docs/manmaster/man3/SHA256_Init.html
//  SHA256_CTX are Deprecated functions. ( new EVP_Digest)

#define DATA_VALID_SIZE ( 256 + sizeof(off_t) + HEX_SHA256_HASH_SIZE )
#define UNUSED_DATA_SIZE ( FILE_HEADER_SIZE - DATA_VALID_SIZE)

struct c_sha256header {
        char fname[256];                  // file name
        off_t size;                       // similar to a 32-bit integer
        char hash[HEX_SHA256_HASH_SIZE];   // hash code of file fname
(hexadecimal string)
        mode_t permission; //permisos del archivo
        // to complete in subsequent versions of the project
        char unused[UNUSED_DATA_SIZE];
};

/**
* end @file s_my_sha256header.h
**/


VALORES DE SALIDA
       En las siguientes situaciones no creará el fichero_destino de
repositorio
       y devolverá un código de error, informando además por la salida
estándar
       de errores un mensaje indicando el tipo de error:

          1: Número de argumentos erróneo.
          2: No puede abrir el fichero origen.
          3: No puede leer del fichero origen.
          4: No puede abrir/crear el fichero destino.
          5: Otro tipo de errores (especificar).
```

6: Otro tipo de errores (especificar).
...
En caso contrario (si no hay errores) devuelve 0.

COMPATIBILIDAD
mysha256_repo debería funcionar en cualquier sistema UNIX.
La firma sha256 generada del fichero de entrada debe ser idéntica
a la firma generada con el comando sha256sum de Linux.

VEASE TAMBIEN
cp(1), open(2), stee(ISO), sha256sum(1), sha(3), SHA256 (3ssl)

AUTOR
Ander Serrano, Mikel Leon y Koldo Intxausti