

U7-ADMINISTRACIÓ DE SISTEMA OPERATIUS

Comprovar sha256sum

1 CODI HASH

Un codi hash és un valor únic generat a partir de dades mitjançant un algorisme matemàtic. Serveix per identificar i verificar informació sense revelar-ne el contingut.

1.1 Característiques:

- De mida fixa (ex: 256 bits per SHA-256).
- Un petit canvi a les dades genera un hash completament diferent.
- No es pot revertir (no es pot obtenir l'original des del hash).

1.2 Usos:

- **Verificació de fitxers (integritat)**
- Emmagatzematge segur de contrasenyes.
- Signatures digitals i seguretat informàtica.

Exemples de diferents algorismes:

En negreta resalte el que anem a usar.

Algorisme	Longitud del hash	Seguretat	Ús principal
MD5	128 bits (32 caràcters)	Feble (col·lisions)	Comprovació de fitxers (no segur per criptografia)
SHA-1	160 bits (40 caràcters)	Feble (col·lisions trobades)	Signatures digitals antigues
SHA-256	256 bits (64 caràcters)	Alta	Certificats digitals, blockchain, integritat de dades
SHA-512	512 bits (128 caràcters)	Molt alta	Seguretat avançada
BLAKE2	256-512 bits	Més ràpid que SHA-256	Criptografia moderna
Argon2	Variable	Molt segura	Emmagatzematge de contrasenyes
bcrypt	192 bits	Resistència a atacs de força bruta	Protecció de contrasenyes

2.- SHA256 en LINUX: *sha256sum*



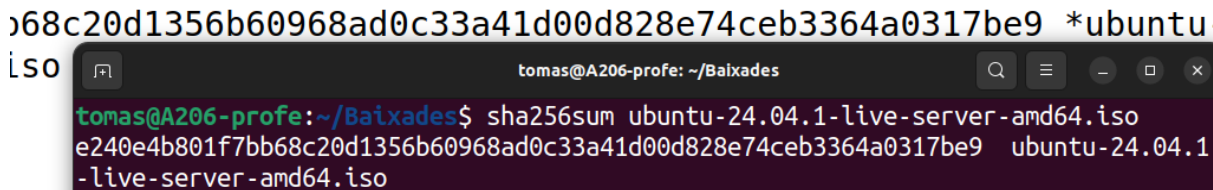
- Llegeix les dades d'un fitxer o entrada.
- Processa les dades mitjançant l'algorisme SHA-256.
- Retorna una cadena hexadecimal de 64 caràcters que representa el hash.

Exemple:

```
sha256sum exemple.txt
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd89c6b247dd60a8a6e  exemple.txt
```

2.1 Verificació de una ISO

Name	Last modified
 Parent Directory	
 SHA256SUMS	2024-08-29 16:08
 <pre>tomas@A206-profe: ~/Baixades tomas@A206-profe:~/Baixades\$ sha256sum ubuntu-24.04.1-live-server-amd64.iso e240e4b801f7bb68c20d1356b60968ad0c33a41d00d828e74ceb3364a0317be9 ubuntu-24.04.1-live-server-amd64.iso</pre>	

3. SHA256 en WINDOWS

3.1 Informació

64-bit Download

✓ Comprueba la descarga

Si quieres comprobar la integridad y autenticidad de los datos de tu descarga, puedes seguir estos pasos:

1. Descarga el archivo ISO del producto deseado y sigue las instrucciones de instalación.
2. Inicia Windows PowerShell. Si necesitas ayuda para encontrar la ubicación de PowerShell para tu sistema operativo, obtén ayuda [aquí](#).
3. En PowerShell, utiliza el cmdlet Get-FileHash para calcular el valor hash del archivo ISO que descargaste. Por ejemplo:
`Get-FileHash C:\Users\user1\Downloads\Contoso8_1_ENT.iso`
4. Si el resultado de SHA256 coincide con el valor de la tabla siguiente para el producto que descargaste, esto confirmará que el archivo no ha resultado dañado, no se ha manipulado ni se ha alterado respecto al original.

3.2 Get-FileHash

```
Get-FileHash -Path "C:\Windows.iso" -Algorithm SHA256
```

Ens donarà, per exemple:

Algorithm	Hash
-----	----
SHA256	0D48C6F236CA9F966ECCD84D9BE01B038516567AABF1C46DCBEE785556B19813

En Windows tenim un codi Hash (sha256) distint per cada idioma:

Esloveno de 32 bits	634B23B37068119A974F6E6155EC663974048A51D0A440B2E6FB8F84E4EEE8E5
Español de 64 bits	0D48C6F236CA9F966ECCD84D9BE01B038516567AABF1C46DCBEE785556B19813
Español de 32 bits	DB414636D7EC65B1AEFCC1242D323E839823DB21FD25A2A9C5DCECC3C16C3309

Comprovem que els codis coincideixen.

4 ALTRES USOS

Encara que el cas de les ISO de Sistemes Operatius serà l'ús més habitual en quant a la verificació de la **integritat d'un fitxer** pode donar altres usos.

Exemple: Ens demanen que compartim en un portal web un fitxer gran que altri podrà descarregar mitjançant https o ftp. Podem generar el codi *sha256* i compartir-lo per a que, després de la descàrrega es puguin comprovar si ha anat bé.

```
tomas@portatil:~$ sha256sum smartgit-linux-23_1_2.tar.gz>>sha256sum.txt
tomas@portatil:~$ ls -l sha256sum.txt
-rw-rw-r-- 1 tomas tomas 95 de gen. 29 12:01 sha256sum.txt
```

És indistint que usem Linux (sha256sum) que usem cmdLets (Get-FileHash). La funció *sha256* és la mateixa.