



## Activitat: hash

En aquesta activitat es practica amb els algorismes de hash

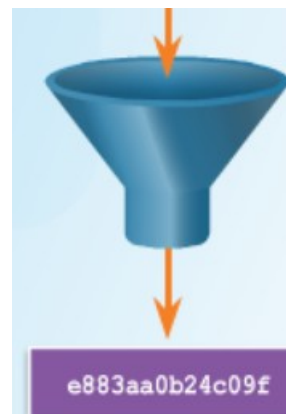
### Hash des de Windows

Programes : HashGenerator, CriptoRes (espanyol), QuickHash, MD5 & SHA Checksum Utility, HashMyFiles, HashTab

### Hash des de Linux

Des de terminal: `sha256sum nomfitxer md5sum , sha1sum , sha512sum`

Des d'entorn gràfic: GtkHash



**Exercici 1.** Comprovar que amb diferents programes (utilitzant la mateixa funció hash sha-256), s'obté el mateix (codi)hash per a un mateix fitxer. Prova amb fitxers xicotets, amb una sola lletra. Prova amb fitxers grans.

**\*\* Prova 2 programes de Windows i 2 programes de Linux (kali)**

**Exercici 2.** Comprovar com canvia el hash canviant només un “bit” d'un fitxer de diversos centenars de Mbytes (512Mbytes = 4.096.000.000 bits)

- Necessitarem una eina de calcule de hash. Tria una.
- Necessitarem un editor hexadecimal per a fer el canvi d'un sol bit. Tria un.

Prenem un fitxer gran. Fem una còpia, li canviem el nom. Comprovem el hash dels dos fitxers. (ha de coincidir)

Prenem el segon fitxer i amb un editor hexadecimal li canviem un sol bit.

Comprovem ara els hash. Observar com ha canviat el hash.

Exemple editor per a windows: Editors per a linux: Ghex, wxHexEditor ...



### HxD Hex Editor

Versión 2.3.0.0 (x86-64)

Copyright © 2002-2019 Maël Hörz

Todos los derechos reservados

[www.mh-nexus.de](http://www.mh-nexus.de)

### wxHexEditor 0.23 Beta for Linux

wxHexEditor es un heditor hexadecimal para GRANDES archivos y dispositivos

© 2006-2012 Erdem U. Altinyurt

<http://www.wxhexeditor.org>



**GHex**

3.18.3

A binary file editor

[GHex Website](http://www.gnome.org/projects/ghex/)

Des de línia de comandos, hexedit, Hexyl, xxd, Hexcurse, Hexer

```
(kali@kali)-[~]
$ sudo apt install hexedit
```

```
00000000  68 6F 6C 61  0A 68 6F 6C  61 0A 68 6F  hola.hola.ho
0000000C  6C 61 0A
00000018
```

Documenta tot el procés i lliura un document en format PDF. Signa'l amb el teu certificat digital. I no oblidis seguir les indicacions del document de Aules “Com fer un treball”