



#HASH

ÍNDICE

1-HASH EN WINDOWS.....	3
1.1-CertUtil.....	3
1.1.1-Generación de hashes.....	3
1.2-HashTab.....	3
1.2.1-Calcular Hash.....	3
1.2.2-Comprobación.....	4
2-HASH EN LINUX.....	5
2.1-Fichero personal.....	5
2.1.1-Generación de hashes.....	5
2.2-Archivo descargado.....	5
2.2.1-Calcular Hash.....	6
2.2.2-Comprobación.....	6
3-COMPARACIÓN DE ALGORITMOS.....	6
3.1-¿Por qué MD5 y SHA-1 no son recomendables?.....	6
3.2-Circunstancias para usar MD5.....	7
4-REFLEXIÓN.....	7

1-HASH EN WINDOWS

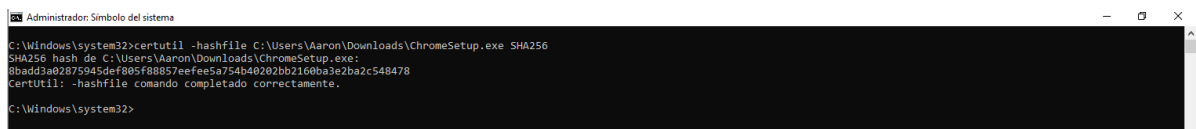
1.1-CertUtil

Es una utilidad de línea de comandos incluida en sistemas Windows, diseñada para gestionar certificados, servicios de certificación y archivos relacionados con la seguridad. Es utilizada principalmente por administradores de sistemas y desarrolladores que trabajan con infraestructura de clave pública (PKI) y certificados digitales.

1.1.1-Generación de hashes

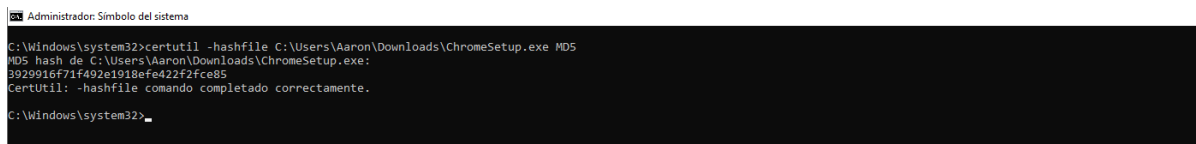
- Sintaxis:
CertUtil -hashfile <ruta_del_archivo> <algoritmo>
 - Ejemplos:

1. SHA256 del instalador de Google Chrome



```
Administrador: Símbolo del sistema
C:\Windows\system32>certutil -hashfile C:\Users\Aaron\Downloads\ChromeSetup.exe SHA256
SHA256 hash de C:\Users\Aaron\Downloads\ChromeSetup.exe:
8badd3a02875945def805f88857eefee5a754b40202bb2160ba3e2ba2c548478
CertUtil: -hashfile comando completado correctamente.
C:\Windows\system32>
```

2. MD5 del instalador de Google Chrome



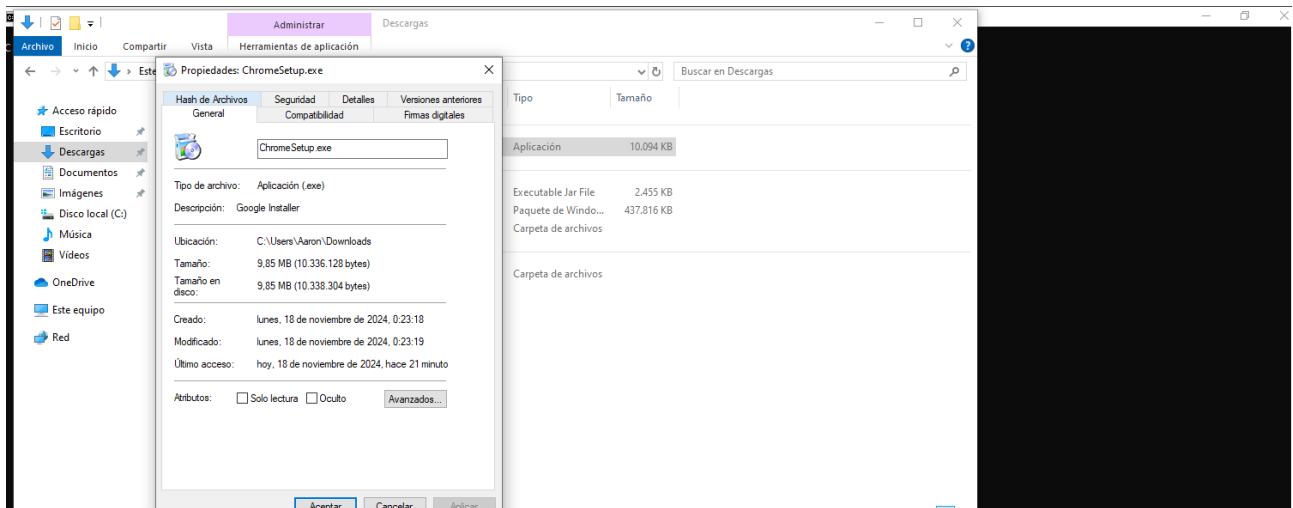
```
Administrador: Símbolo del sistema
C:\Windows\system32>certutil -hashfile C:\Users\Aaron\Downloads\ChromeSetup.exe MD5
MD5 hash de C:\Users\Aaron\Downloads\ChromeSetup.exe:
3929916f71f492e1918efe422f2fce85
CertUtil: -hashfile comando completado correctamente.
C:\Windows\system32>
```

1.2-HashTab

Es una herramienta gratuita para Windows que permite calcular y comparar hashes directamente desde las propiedades de un archivo. Es una solución sencilla para verificar la integridad y autenticidad de archivos descargados u otros datos.

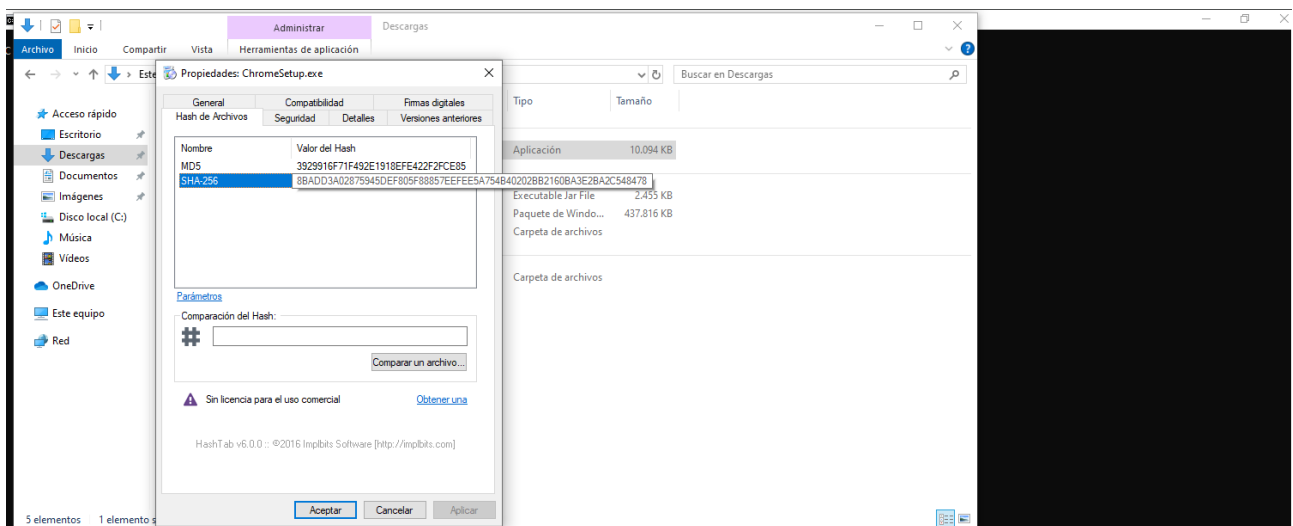
1.2.1-Calcular Hash

Para calcular el hash de un archivo hacemos click derecho en él, vamos a propiedades y en la pestaña de “Hash de Archivos”.

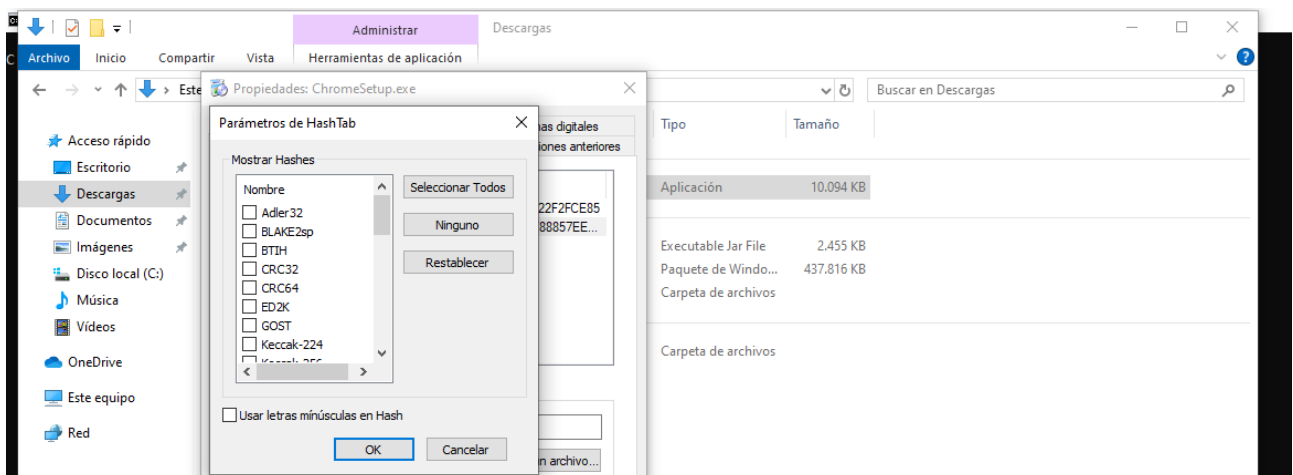


1.2.2-Comprobación

Vemos que el hash que nos da esta aplicación también es el que nos indicaba el comando de CertUtil.



Al hacer click en la opción de Parámetros esta aplicación nos permite añadir o quitar diferentes tipos de hashes existentes.



2-HASH EN LINUX

2.1-Fichero personal

Creamos un fichero con el que realizaremos las pruebas hash.

```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ sudo nano prueba.txt  
aaron@aaron-VirtualBox:~$ cat prueba.txt  
Archivo para realizar la comprobación del hash  
aaron@aaron-VirtualBox:~$
```

2.1.1-Generación de hashes

- Generar hash MD5.

```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ md5sum prueba.txt  
0ce89c26a33307739fde6d167b5d0cd7  prueba.txt  
aaron@aaron-VirtualBox:~$
```

- Generar hash SHA-256.

```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ sha256sum prueba.txt  
7e42c5f8f26b8259c9726c145f1eae07ce9e3d4870c28f59b8a88e28d129aca0  prueba.txt  
aaron@aaron-VirtualBox:~$
```

2.2-Archivo descargado

Antes de descargar el archivo, el proveedor del archivo puede proporcionar el hash. Esto generalmente aparece junto al enlace de descarga y luce como un código largo, por ejemplo:

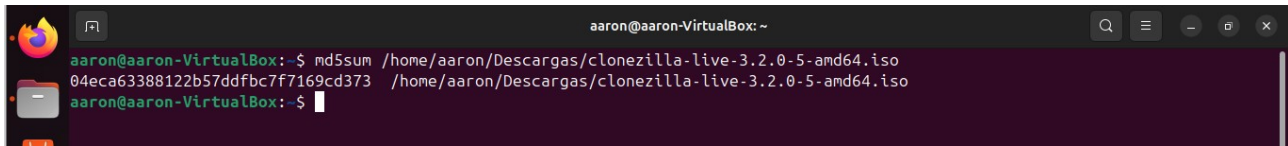
The screenshot shows the Clonezilla website's checksums page. The browser address bar displays `https://clonezilla.org/downloads/stable/checksums.php`. The page header includes the Clonezilla logo and navigation links for software, disk imaging, cloning, live system, and backup software. A sidebar on the left contains links for About, News, Screenshots, Live CD/USB, Live Docs, Server Edition, Download, CD/USB key vendors, DRBL-wlnroll, Related LiveCD, Testimonials, Lecture Materials, Related Articles, Partners, FAQ/Q&A, Forum, Mailing Lists, Developers, Contributors, Related links, and Local communities. The main content area lists MD5SUMS, SHA1SUMS, and SHA256SUMS for various Clonezilla live system files. The SHA256SUMS section is expanded, showing a long list of file names and their corresponding 64-character hash values.

File Name	SHA256 Hash
clonezilla-live-3.2.0-5-amd64.iso	2748505fb76346a473d7a27413186abd1c999367b5ba1d209b07168f9703495
clonezilla-live-3.2.0-5-i686.iso	6361384bf0d6a71341b53e106f72b3247b57abcfab6b5b0a8ea33a3c5927113
clonezilla-live-3.2.0-5-i686-pae.iso	9e1ed99a344f971a47241e8574263b4d1b40b0db4dd936845f6c53f65f0bba4
clonezilla-live-3.2.0-5-amd64.zip	96a7468bce45c380b47c2769eb89d5e40b5536362219359f7a304c0f6fdd6509
clonezilla-live-3.2.0-5-i686-pae.zip	002bf772a666bbe0c1aa904c6c8d4af97cfff4edf99a9142c145113189528c7d2
clonezilla-live-3.2.0-5-i686-pae.zip	1907db5afa6ac73f41a6eb04731d6e9899e98a70b32adc94931bd5c1dff6cb8b

En esta práctica descargaré clonezilla, la versión será la stable(3.2.0-5), la arquitectura de CPU será amd64 y el tipo de fichero será ISO.

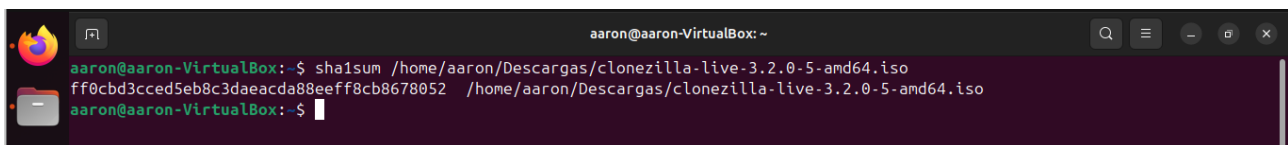
2.2.1-Calcular Hash

- Hash MD5



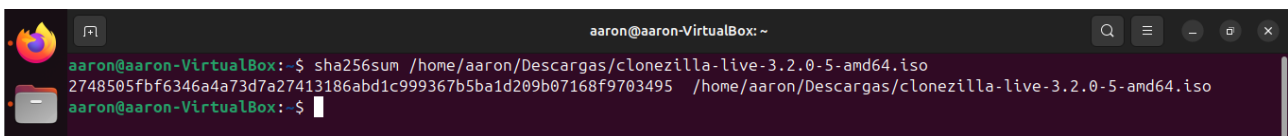
```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ md5sum /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
04eca63388122b57ddfb7f7169cd373 /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
aaron@aaron-VirtualBox:~$
```

- Hash SHA-1



```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ sha1sum /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
ff0cbd3cced5eb8c3daeacda88eeff8cb8678052 /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
aaron@aaron-VirtualBox:~$
```

- Hash SHA-256



```
aaron@aaron-VirtualBox: ~  
aaron@aaron-VirtualBox:~$ sha256sum /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
2748505fbf6346a4a73d7a27413186abd1c999367b5ba1d209b07168f9703495 /home/aaron/Descargas/clonezilla-live-3.2.0-5-amd64.iso  
aaron@aaron-VirtualBox:~$
```

2.2.2-Comprobación

Comparamos el hash que hemos generado con el que proporciona el proveedor. Si coinciden, significa que el archivo es íntegro y no ha sido modificado.

Si no coinciden, es posible que el fichero haya recibido alteraciones maliciosas.

3-COMPARACIÓN DE ALGORITMOS

3.1-¿Por qué MD5 y SHA-1 no son recomendables?

Estos algoritmos ya no se recomiendan para aplicaciones críticas debido a sus vulnerabilidades a ataques de colisión. Una colisión ocurre cuando dos entradas diferentes producen el mismo valor de hash, lo que compromete la seguridad del sistema.

Para aplicaciones críticas, se recomienda usar algoritmos más seguros como SHA-256 o SHA-512, que tienen una mayor resistencia a los ataques de colisión

- Ejemplo:

Imaginemos que un banco utiliza MD5 para almacenar contraseñas de los usuarios. Un atacante podría generar dos contraseñas diferentes que produzcan el mismo hash MD5. Si el atacante obtiene acceso a la base de datos y encuentra una de estas contraseñas, podría usarla para acceder a las cuentas de los usuarios, ya que el sistema no distinguiría entre las dos contraseñas.

3.2-Circunstancias para usar MD5

- Verificación de integridad no crítica:
 - Uso: Comparar rápidamente si dos archivos son idénticos.
 - Ejemplo: Poder detectar si hay archivos duplicados.
- Indexación o generación de identificadores:
 - Uso: Como un mecanismo rápido para generar identificadores únicos para datos (en un entorno controlado).
 - Ejemplo: Asignar claves únicas para imágenes en una base de datos local.
- Aplicaciones internas sin exposición a amenazas externas:
 - Uso: En sistemas internos donde no existe un riesgo significativo de ataque.
 - Ejemplo: En un laboratorio de pruebas.

4-REFLEXIÓN

Las funciones hash son fundamentales en la seguridad informática porque garantizan la integridad, autenticidad y confidencialidad de los datos. Actúan como "huellas digitales" únicas para archivos o mensajes, permitiendo detectar cualquier alteración, por mínima que sea.

Su uso es esencial en aplicaciones como firmas digitales, almacenamiento seguro de contraseñas y verificación de integridad de datos. Sin embargo, su efectividad depende de la robustez del algoritmo. Si una función hash es vulnerable a colisiones, la seguridad del sistema entero puede quedar comprometido. Por ello, elegir algoritmos seguros y actualizados es crucial para proteger la información.