

## Informe de Laboratorio #1:

### Herramientas para el cálculo de valores hash

Nombre	Identificación
Santiago Poveda Garcia	CC: 1005099004

#### 1 Herramienta online para calcular valores hash

Carlos: Diplomado Gestión de infraestructura de TI aplicada a entornos empresariales con una perspectiva desde la seguridad de informática.  
Julio 12 de 2024

\*Escriba su nombre \*Escriba la fecha

Haga clic en el botón **Calculate SHA256 hash**. Escriba aquí el resultado.

75893112a0bddf28911da5625ce73f4e3896ebc60820fde0a95ec38638c6fc58

Complete la siguiente tabla acerca del resultado del hash SHA256:

Cantidad de bytes	32	Cantidad de dígitos hexadecimales	64
-------------------	----	-----------------------------------	----

Utilice el algoritmo MD5. Escriba aquí el resultado.

bd6b2f26d8182b03698ddac8dcb55011

Complete la siguiente tabla acerca del resultado del hash MD5:

Cantidad de bytes	16	Cantidad de dígitos hexadecimales	32
-------------------	----	-----------------------------------	----

Utilice el algoritmo SHA-1. Escriba aquí el resultado.

f7dcdeab9a4963efa6eee161104d751994fedca0

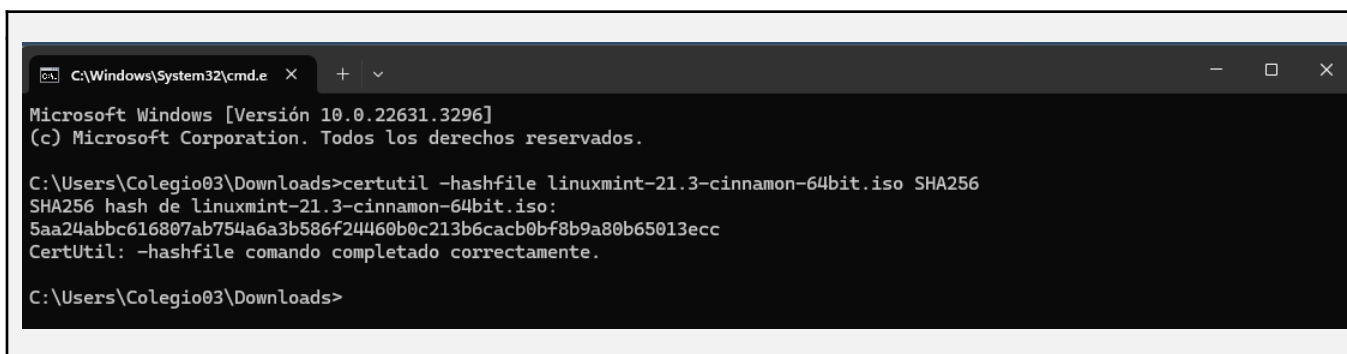
Complete la siguiente tabla acerca del resultado del hash SHA-1:

Cantidad de bytes	20	Cantidad de dígitos hexadecimales	40
-------------------	----	-----------------------------------	----

## 2 Herramienta CLI para calcular valores hash en Windows

Calcule el valor hash del archivo *linuxmint-21.3-cinnamon-64bit.iso* mediante el comando **CertUtil** usando el algoritmo SHA-256.

Agregue aquí una captura de pantalla.



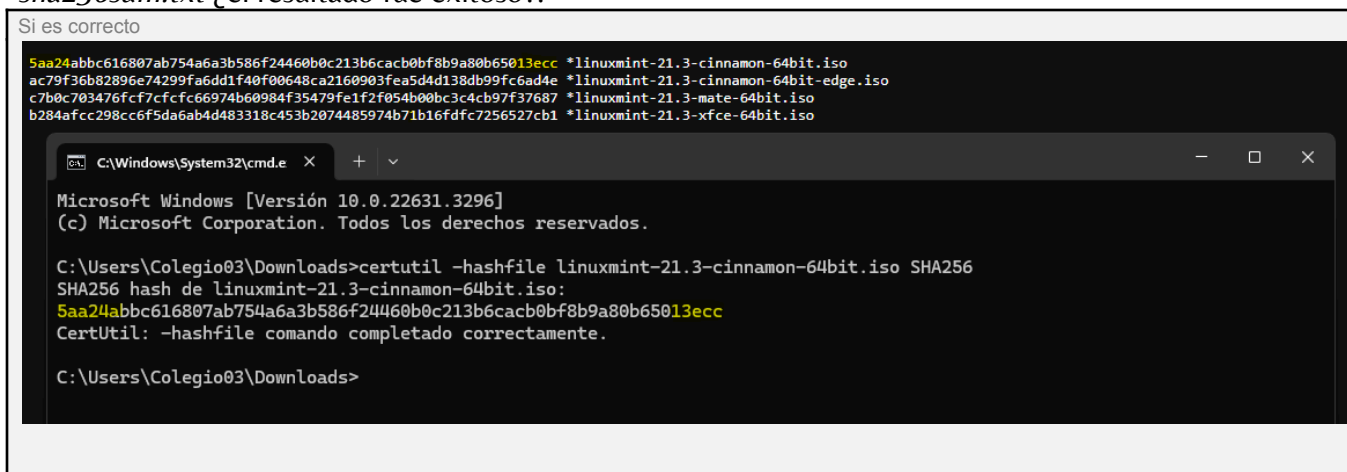
```

C:\Windows\System32\cmd.e  X  +  v
Microsoft Windows [Versión 10.0.22631.3296]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Colegio03\Downloads>certutil -hashfile linuxmint-21.3-cinnamon-64bit.iso SHA256
SHA256 hash de linuxmint-21.3-cinnamon-64bit.iso:
5aa24abbc616807ab754a6a3b586f24460b0c213b6cacb0bf8b9a80b65013ecc
CertUtil: -hashfile comando completado correctamente.

C:\Users\Colegio03\Downloads>
  
```

Al comparar el hash calculado a partir del archivo descargado con el hash incluido en el archivo *sha256sum.txt* ¿el resultado fue exitoso?:



```

Si es correcto

5aa24abbc616807ab754a6a3b586f24460b0c213b6cacb0bf8b9a80b65013ecc *linuxmint-21.3-cinnamon-64bit.iso
ac79f36b82896e74299fa6dd1f40f00648ca2160903fea5d4d138db99fc6ad4e *linuxmint-21.3-cinnamon-64bit-edge.iso
c7b0c703476fc7cfcfc66974b60984f35479fe1f2f054b00bc3c4cb97f37687 *linuxmint-21.3-mate-64bit.iso
b284afcc298cc6f5da6ab4d483318c453b2074485974b71b16dfc7256527cb1 *linuxmint-21.3-xfce-64bit.iso

C:\Windows\System32\cmd.e  X  +  v
Microsoft Windows [Versión 10.0.22631.3296]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Colegio03\Downloads>certutil -hashfile linuxmint-21.3-cinnamon-64bit.iso SHA256
SHA256 hash de linuxmint-21.3-cinnamon-64bit.iso:
5aa24abbc616807ab754a6a3b586f24460b0c213b6cacb0bf8b9a80b65013ecc
CertUtil: -hashfile comando completado correctamente.

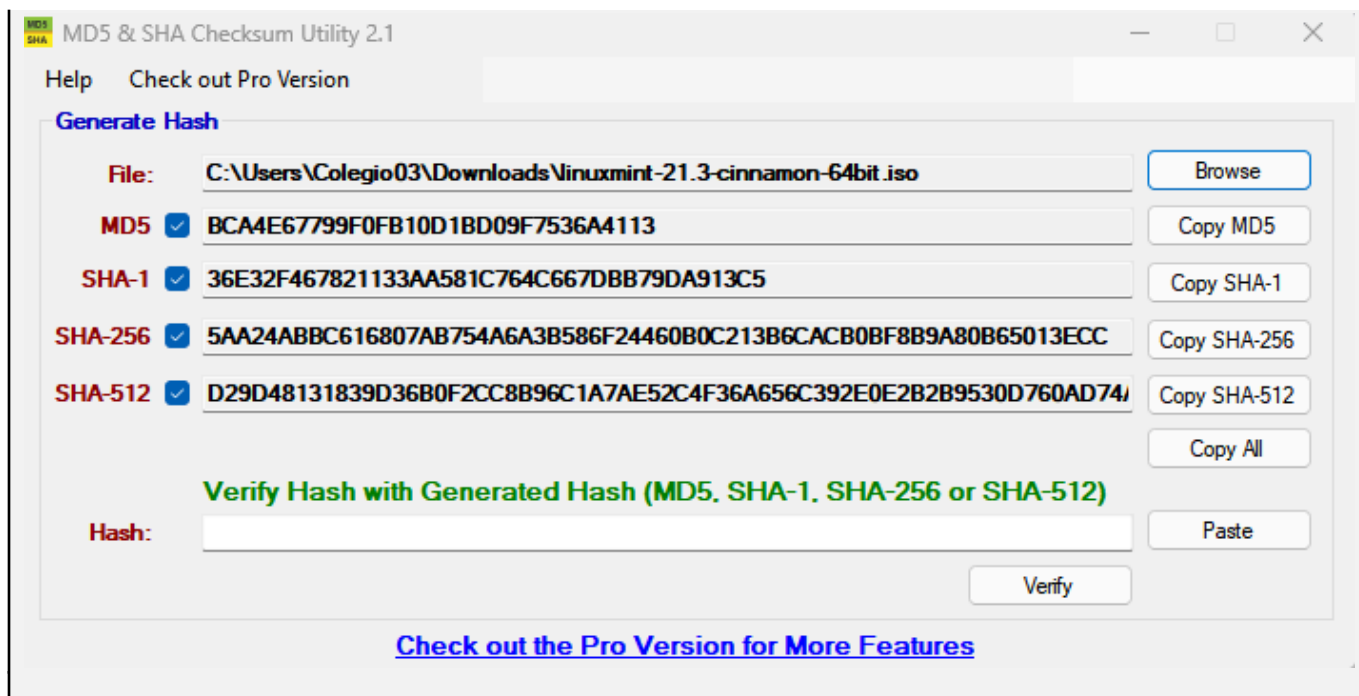
C:\Users\Colegio03\Downloads>
  
```

## 3 Herramienta GUI para calcular valores hash en Windows

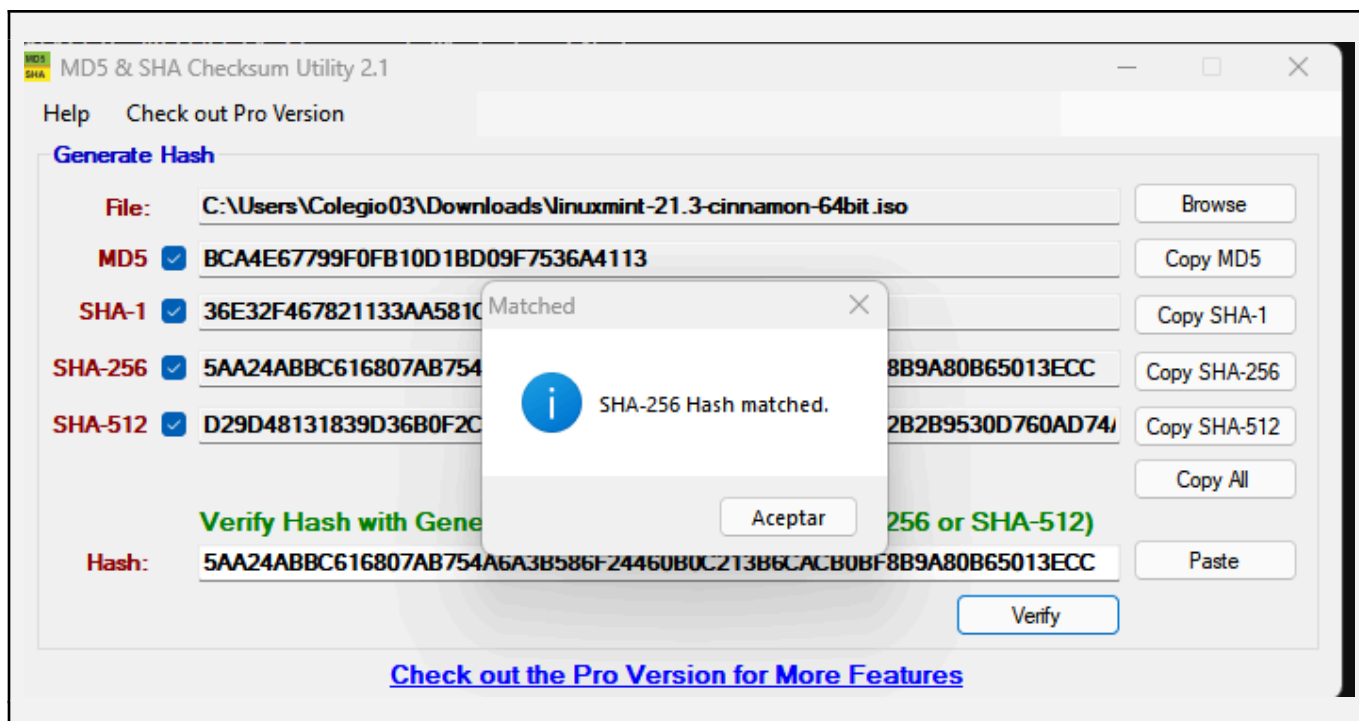
Usando la aplicación *MD5 & SHA Checksum Utility 2.1*, calcule el valor de hash para el archivo descargado con la imagen .iso de *Linux Mint 21.3* utilizada en el punto anterior.

Agregue aquí una captura de pantalla.

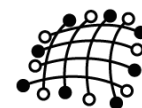




Verifique el valor del SHA-256 obtenido con la herramienta *MD5 & SHA Checksum Utility 2.1* agregando en la sección de verificación el hash incluido en el archivo *sha256sum.txt*. Agregue aquí una captura de pantalla.



#### 4 Herramienta CLI para calcular valores hash en Linux y Mac OS X



En una máquina virtual de Linux Mint 21.3:

a) Calcular el SHA 256 a un archivo.

Descargue o copie los archivos *linuxmint-21.3-cinnamon-64bit.iso* y *sha256sum.txt*.

Calcule el valor hash del archivo *linuxmint-21.3-cinnamon-64bit.iso* mediante el comando **shasum** usando el algoritmo SHA-256.

Agregue aquí una captura de pantalla.

```
i7savage@i7savage-VirtualBox:~/Desktop$ shasum -a 256 linuxmint-21.3-cinnamon-64bit.iso
5aa24abbc616807ab754a6a3b586f24460b0c213b6cacb0bf8b9a80b65013ecc linuxmint-21.3-cinnamon-64bit.iso
i7savage@i7savage-VirtualBox:~/Desktop$
```

Haga una verificación visual del hash obtenido. ¿Corresponde al valor incluido en el archivo *sha256sum.txt*?

Si corresponde.

b) Verificar la integridad de un archivo a partir de un valor de integridad almacenado en un archivo.

Verifique los valores hash incluidos en el archivo *sha256sum.txt* mediante el comando **shasum** usando el algoritmo SHA-256.

Agregue aquí una captura de pantalla.

```
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 -c sha256sum.txt
linuxmint-21.3-cinnamon-64bit.iso: OK
```

## Ejercicio

En una carpeta, copiar cuatro archivos binarios, los cuales pueden ser *.pdf* o imágenes *.jpg*, *.jpeg* o *.png*. Crear el archivo *hash.txt* con los valores de hash para los cuatro archivos al usar el algoritmo SHA-256. Utilice el comando **shasum** calcular y agregar el hash correspondiente al archivo especificado, al final del archivo *hash.txt*.

Agregue aquí una captura de pantalla.

```
i7savage@i7savage-VirtualBox:~/Desktop$ mkdir lab1
i7savage@i7savage-VirtualBox:~/Desktop$ ls
lab1  linuxmint-21.3-cinnamon-64bit.iso
i7savage@i7savage-VirtualBox:~/Desktop$ cd lab1
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 1.jpeg >> hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 2.jpeg >> hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 3.jpeg >> hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ ls
1.jpeg 2.jpeg 3.jpeg 4.pdf hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 4.pdf >> hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ cat hash.txt
c14e76946d761b9c4be4944352a0f0ad4b27b3f75fec4c5467410840e138ac5a 1.jpeg
fe7f1b3b7a8d7bd2f3f7e4231cc09b4c342d9c74d8209dcfaa608232b4892ced 2.jpeg
0dc84946417e61bd8c770c61c87f757b70ffa4d045fcc20a6cb3697b3037f7eb 3.jpeg
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855 4.pdf
i7savage@i7savage-VirtualBox:~/Desktop/lab1$
```

Repita el mismo procedimiento con los demás archivos de la carpeta o utilice expresiones regulares con comodines.

Agregue aquí una captura de pantalla con el contenido del archivo *hash.txt*.

```
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 *.jpeg *.pdf >> hash.txt
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ cat hash.txt
c14e76946d761b9c4be4944352a0f0ad4b27b3f75fec4c5467410840e138ac5a 1.jpeg
fe7f1b3b7a8d7bd2f3f7e4231cc09b4c342d9c74d8209dcfaa608232b4892ced 2.jpeg
0dc84946417e61bd8c770c61c87f757b70ffa4d045fcc20a6cb3697b3037f7eb 3.jpeg
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855 4.pdf
c14e76946d761b9c4be4944352a0f0ad4b27b3f75fec4c5467410840e138ac5a 1.jpeg
fe7f1b3b7a8d7bd2f3f7e4231cc09b4c342d9c74d8209dcfaa608232b4892ced 2.jpeg
0dc84946417e61bd8c770c61c87f757b70ffa4d045fcc20a6cb3697b3037f7eb 3.jpeg
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855 4.pdf
i7savage@i7savage-VirtualBox:~/Desktop/lab1$
```

Verifique el hash SHA-256 de todos los archivos relacionados en el archivo *hash.txt*. Utilice el comando *shasum*.

Agregue aquí una captura de pantalla de la verificación usando el archivo *hash.txt*.



```
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 -c hash.txt
1.jpeg: OK
2.jpeg: OK
3.jpeg: OK
4.pdf: OK
1.jpeg: OK
2.jpeg: OK
3.jpeg: OK
4.pdf: OK
i7savage@i7savage-VirtualBox:~/Desktop/lab1$
```

Modifique el archivo *hash.txt*, de manera que dos de los valores de hash sean alterados. Repita el comando anterior.

Agregue aquí una captura de pantalla de la verificación usando el archivo *hash.txt* luego de alterar algunos valores hash.

```
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 -c hash.txt
1.jpeg: FAILED
2.jpeg: OK
3.jpeg: OK
4.pdf: FAILED
1.jpeg: OK
2.jpeg: OK
3.jpeg: OK
4.pdf: OK
shasum: WARNING: 2 computed checksums did NOT match
i7savage@i7savage-VirtualBox:~/Desktop/lab1$
```

Modifique el archivo *hash.txt*, de manera que se agreguen manualmente dos líneas con valores de hash ficticios que hagan referencia a archivos que no están en el directorio de trabajo. Repita el comando anterior.

Agregue aquí una captura de pantalla de la verificación usando el archivo *hash.txt* luego de incluir valores de hash para archivos inexistentes en la carpeta.



```
i7savage@i7savage-VirtualBox:~/Desktop/lab1$ shasum -a 256 -c hash.txt
1.jpeg: FAILED
2.jpeg: OK
3.jpeg: OK
4.pdf: FAILED
1.jpeg: OK
2.jpeg: OK
3.jpeg: OK
4.pdf: OK
shasum: 5.jpeg: No such file or directory
5.jpeg: FAILED open or read
shasum: WARNING: 1 line is improperly formatted
shasum: WARNING: 1 listed file could not be read
shasum: WARNING: 2 computed checksums did NOT match
i7savage@i7savage-VirtualBox:~/Desktop/lab1$
```