

* **GRACE OSEKO**
* **658483**
* **FIC4050: COMPUTER FORENSICS AND INVESTIGATION**
* **LAB: HASHING**

# Activity 8-1: Hashing Individual Files Comparison

## HashCalc main exercise

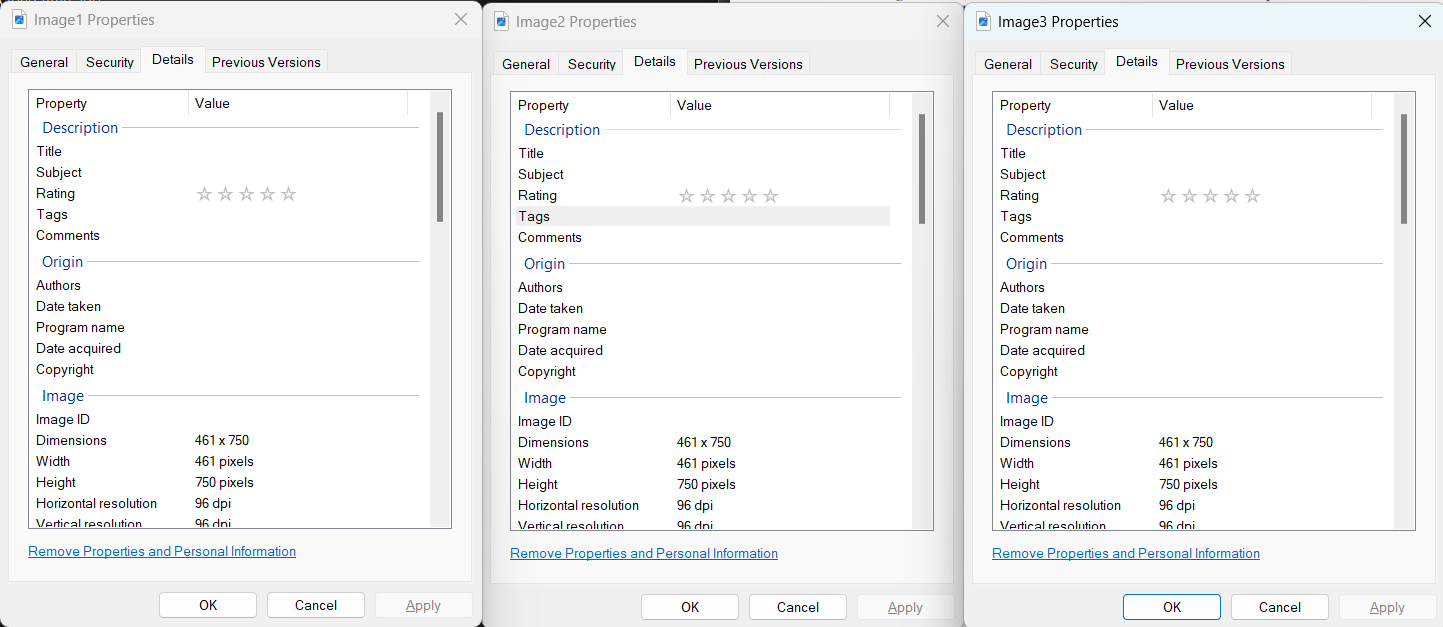
Tools used **HashCalc**

Dataset used **File\_Hashing\_1.zip**

HashCalc successfully installed

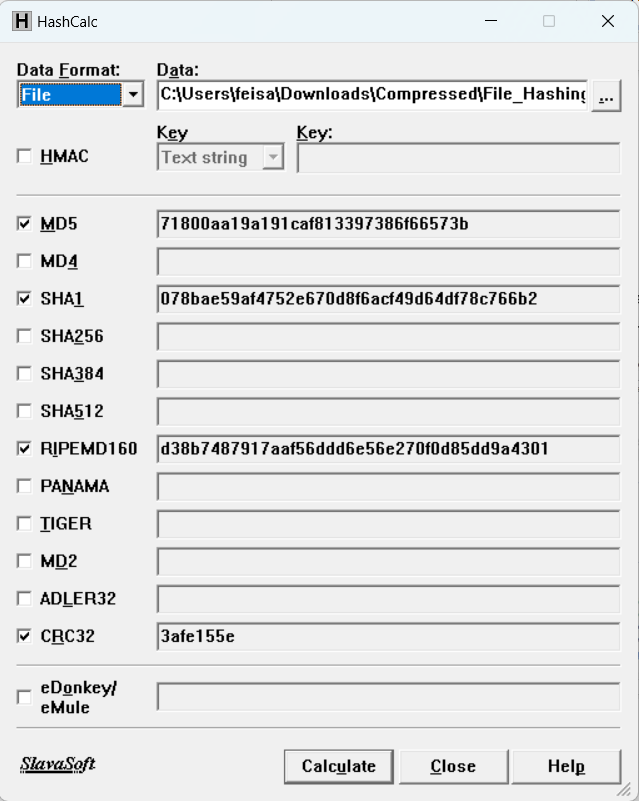
File\_Hashing\_1.zip successfully downloaded

Unzipped contents of above using the password “hands-on”



Properties (details) showed above

HashCalc successfully opened

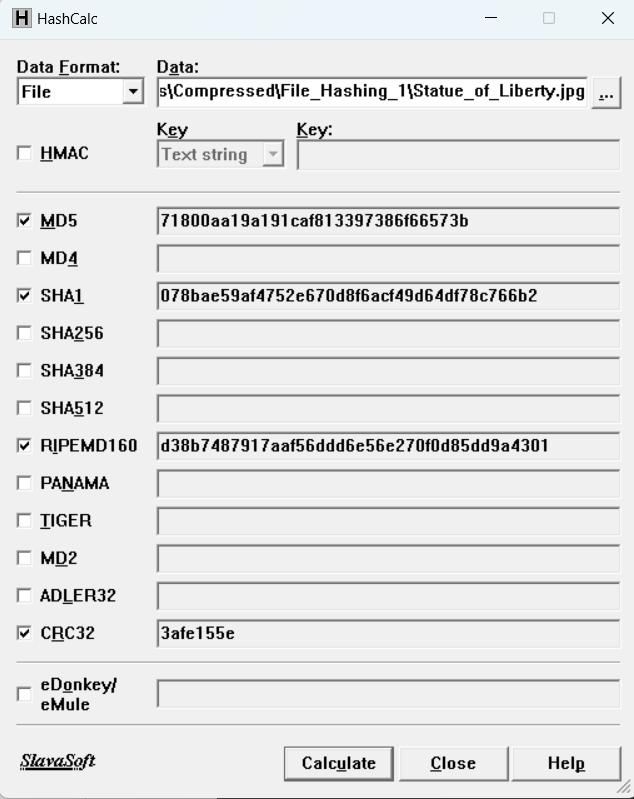


Hash values are as above of Image1.

The MD5 hash value is 71800aa19a191caf813397386f66573b

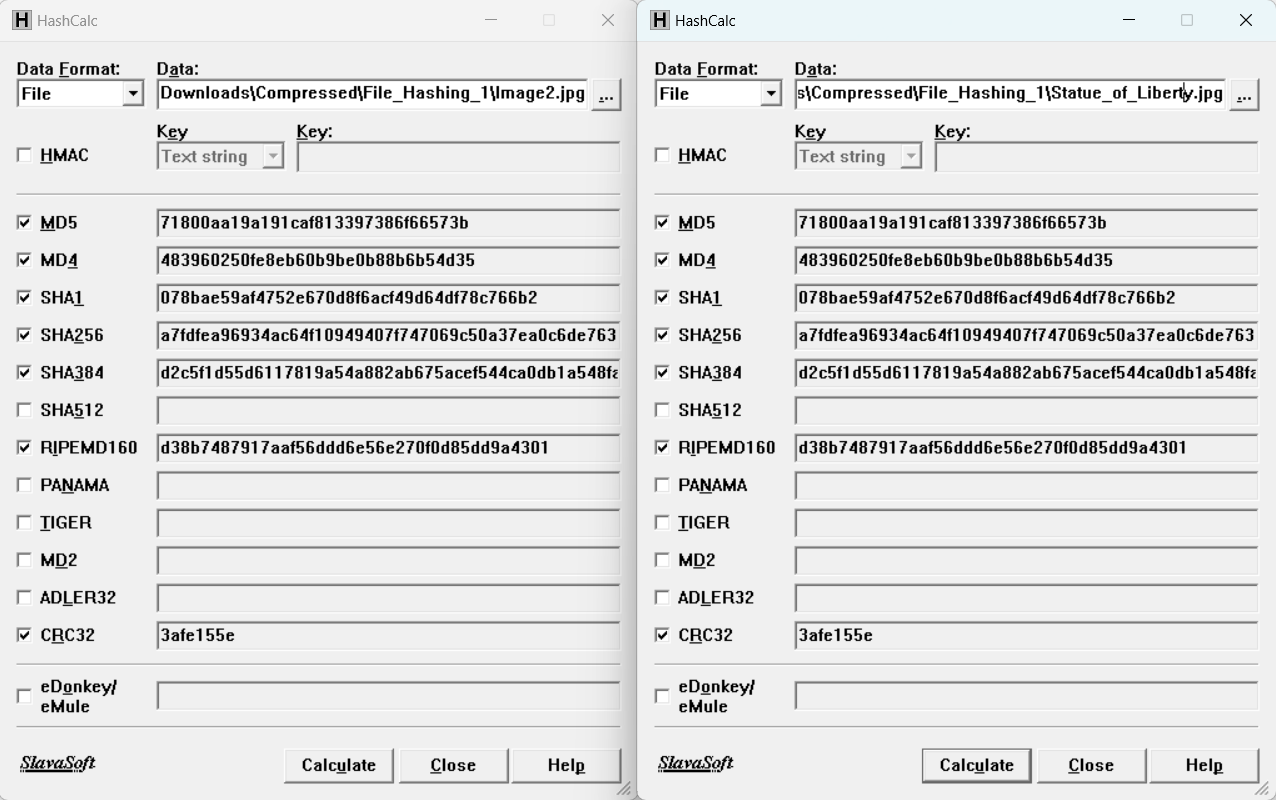
Image1.jpg successfully changed to “Statue\_of\_Liberty.jpg.”





Hash value of the renamed file is the same 71800aa19a191caf813397386f66573b

This is because the hash value is dependent on the content and not the metadata of a file which is safer as the hash value wouldn’t change by simply renaming files



Hash values for Image2 and Image3 are as above

The renamed file originally Image1 and Image2 are the same as all the hash values are the same e.g.

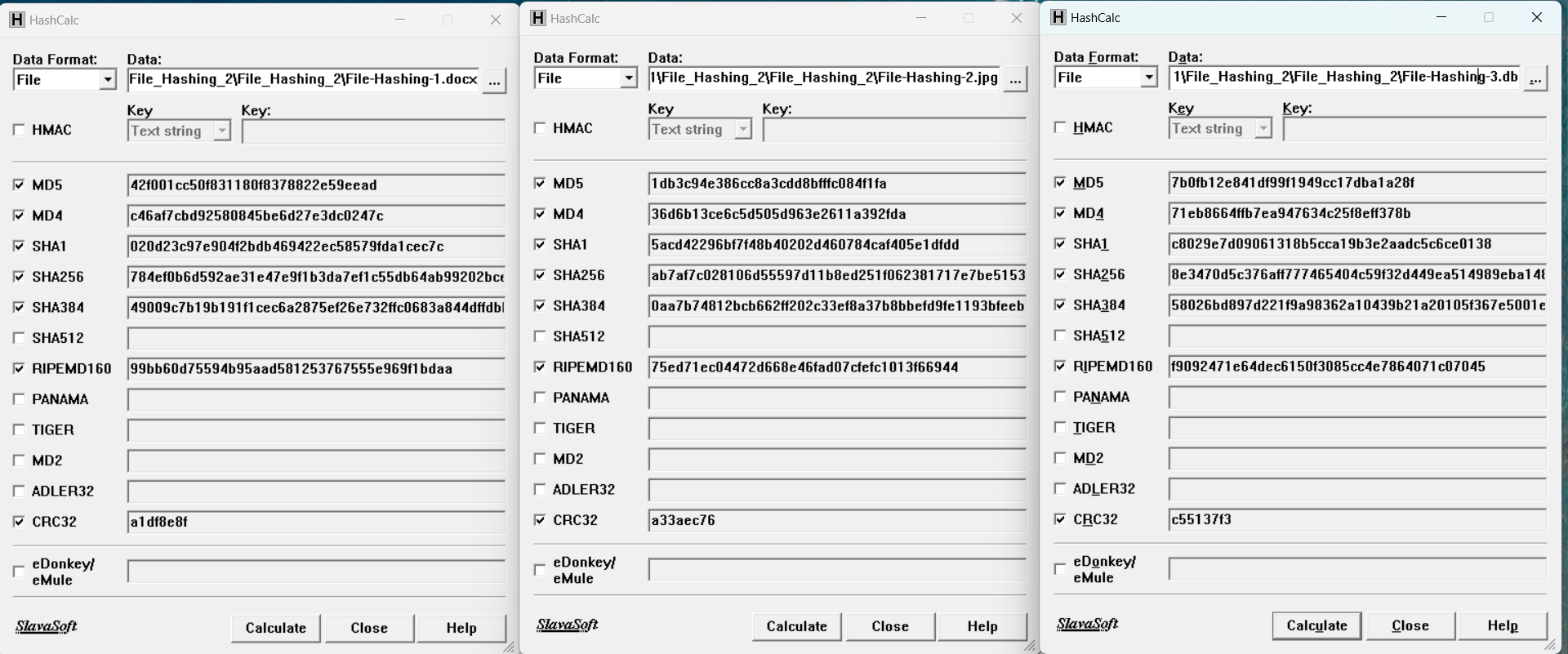
SHA256 are a7fdfea96934ac64f10949407f747069c50a37ea0c6de76315660f33350cf372

## Additional Exercise

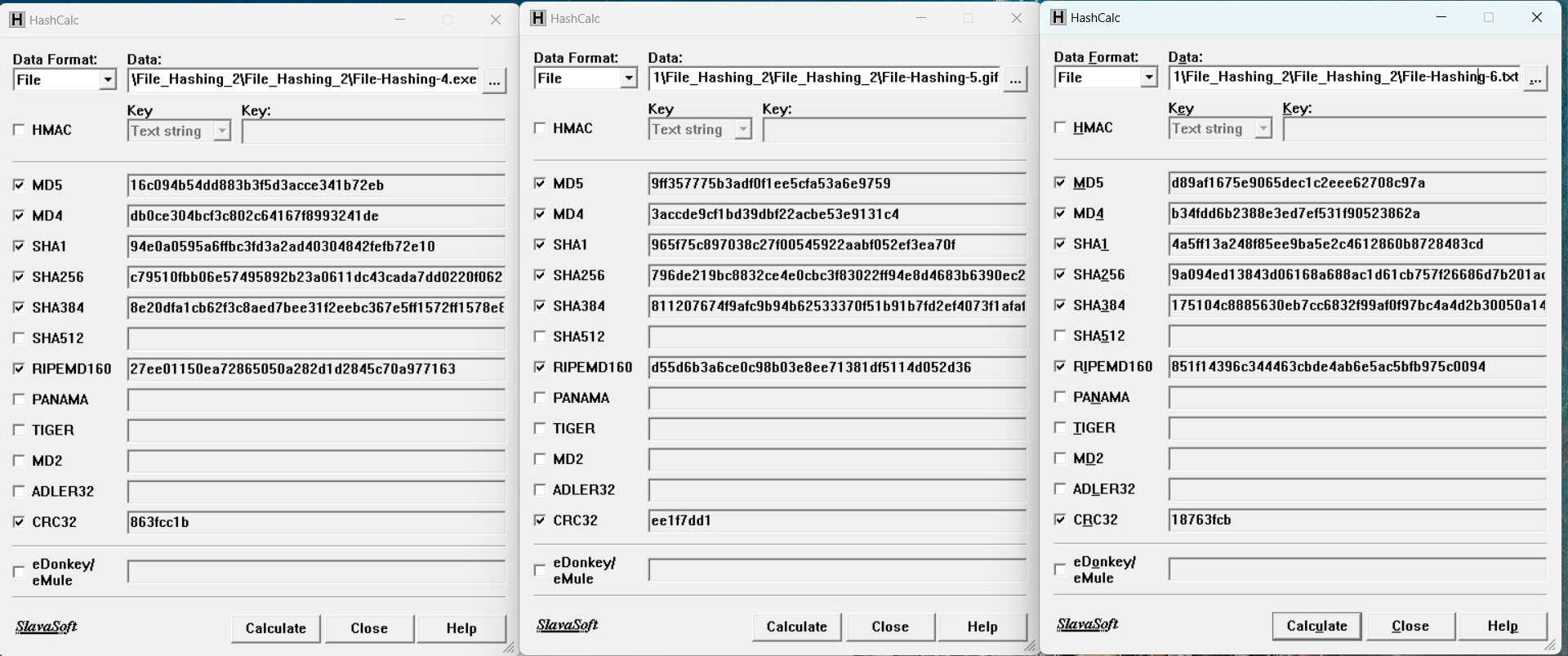
Dataset used **File\_Hashing\_2.zip**

File\_Hashing\_2.zip successfully downloaded

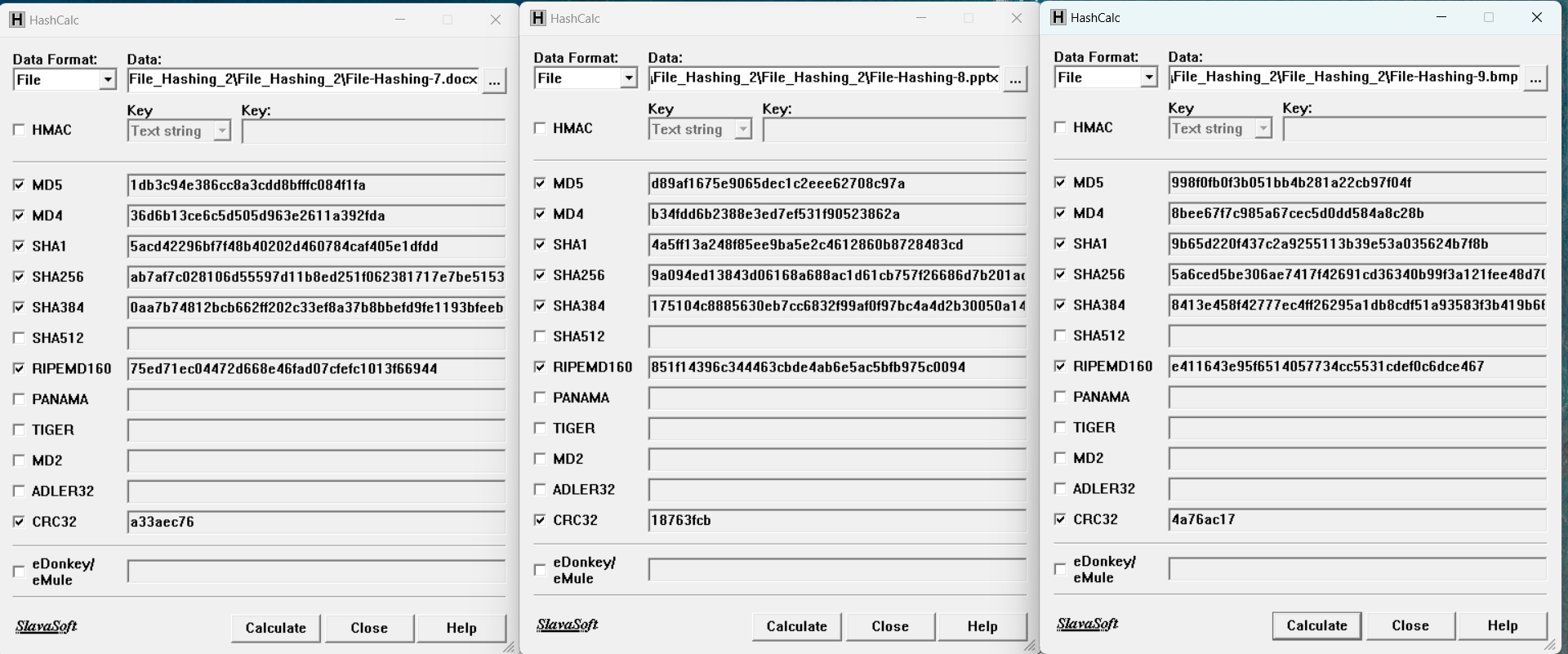
Unzipped contents of above using the password “hands-on”



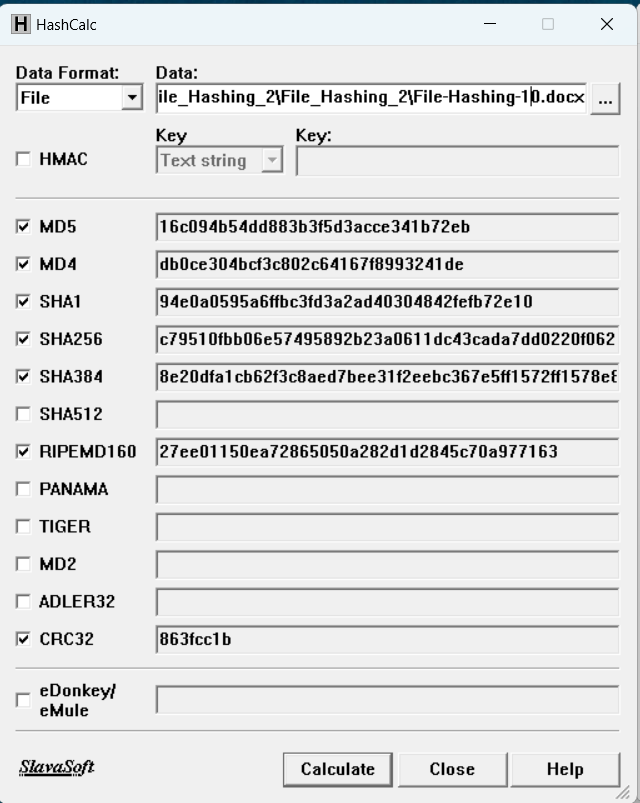
Hash values above for files 1,2,3

****

Hash values above for files 4,5,6



Hash values above for files 7,8,9

**Files 2 and 7 are the same**

MD5 hash is 1db3c94e386cc8a3cdd8bfffc084f1fa

**Files 4 and 10 are the same**

MD5 hash is 16c094b54dd883b3f5d3acce341b72eb

**Files 6 and 8 are the same**

MD5 hash is d89af1675e9065dec1c2eee62708c97a

**This tells us that the type of file (extension) does not matter the hash values can still be same**

Hash values above for file 10

# Activity 8-2: Hashing Folders and Their Contents for Comparison and Searching

## HashMyFiles main exercise

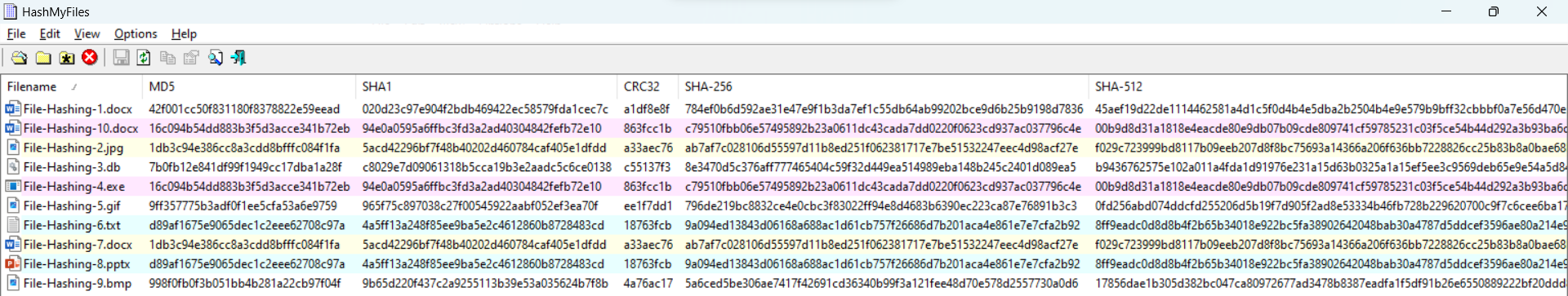
Tools used **HashMyFiles**

Dataset used **File\_Hashing\_2.zip and File\_Hashing\_3.zip**

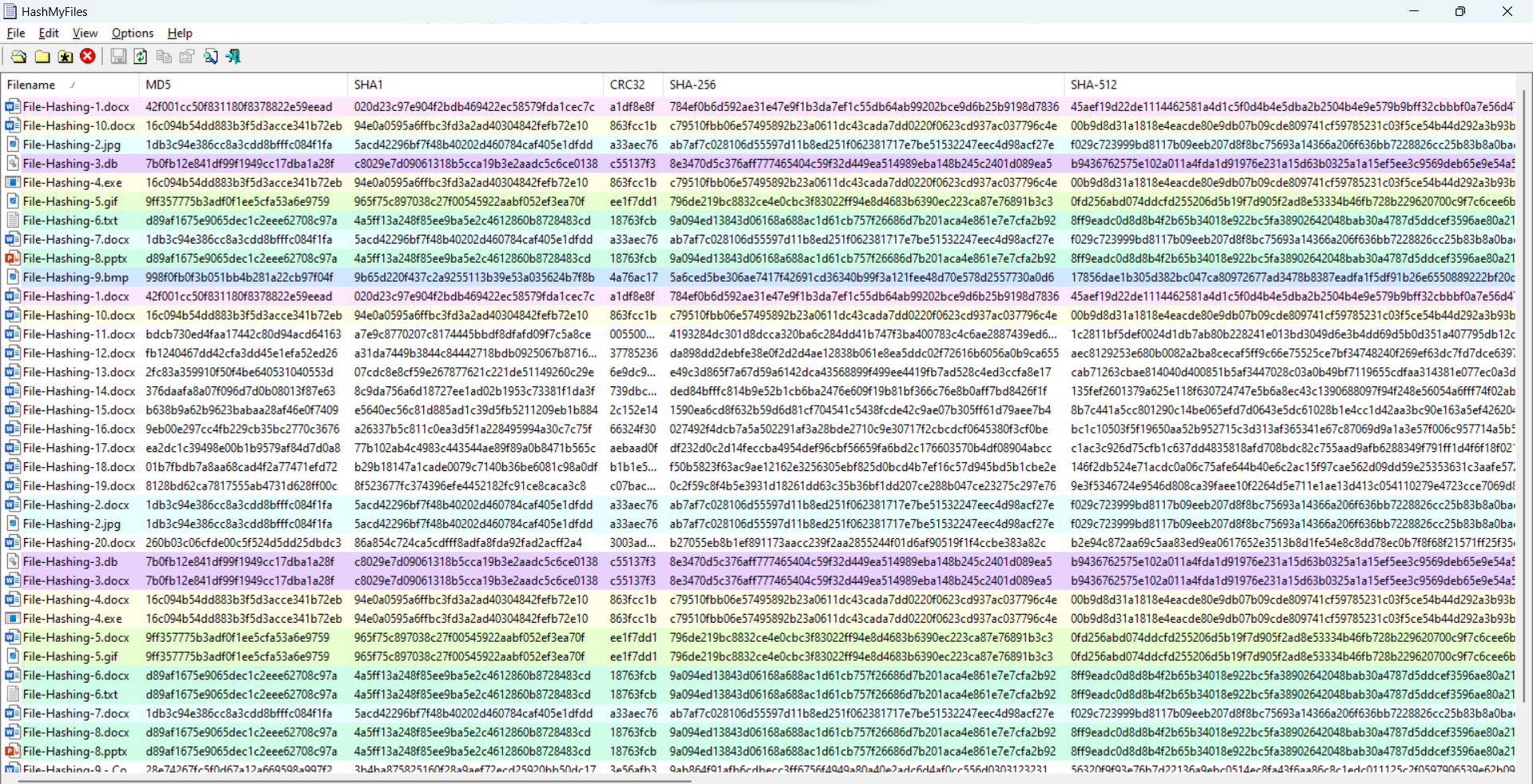
HashMyFiles successfully installed and launched

File\_Hashing\_2.zip and File\_Hashing\_3.zip successfully downloaded

Unzipped contents of above using the password “hands-on”

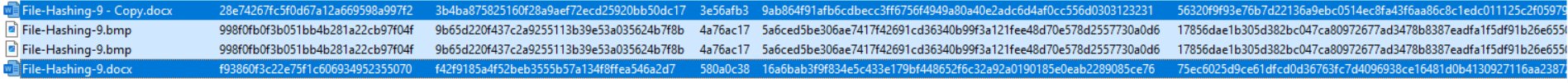


The above were the hash files for the content of File\_Hashing\_2 folder



The hash files for contents of File\_Hashing\_3 folder was appended to the list

 38 files in total have been hashed



File-Hashing-9.docx MD5 hash value is : **f93860f3c22e75f1c606934952355070**

File-Hashing-9 - Copy.docx MD5 hash value is : **28e74267fc5f0d67a12a669598a997f2**

The files “File-Hashing-9.docx” and “File-Hashing-9 - Copy.docx” do not have the same hash values meaning that the contents of the files are different and that the file has been altered in some way

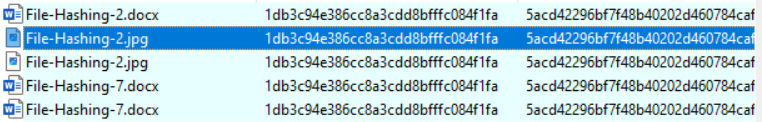
Searched for the hash value b638b9a62b9623babaa28af46e0f7409 and got the following result



This shows that File-Hashing-15.docx has the hash value b638b9a62b9623babaa28af46e0f7409

## Additional Exercise

Searched for the hash value 1db3c94e386cc8a3cdd8bfffc084f1fa and got the following result



This shows that the hash value 1db3c94e386cc8a3cdd8bfffc084f1fa are being shared by the following files

File-Hashing-2.docx from File\_Hashing\_3 folder

File-Hashing-2.jpg from File\_Hashing\_2 folder

File-Hashing-2.jpg from File\_Hashing\_3 folder

File-Hashing-7.docx from File\_Hashing\_2 folder

File-Hashing-7.docx from File\_Hashing\_3 folder

Searched for the hash value a26337b5c811c0ea3d5f1a228495984a30c7c75f and got no result, there is no file that has that hash value. There is File-Hashing-16.docx that has a very similar hash value however a digit is different

# Activity 8-3: Hashing Evidence Files for Validation

## HashCalc and FTK Imager main exercise

Tools used **HashCalc and FTK Imager**

Forensic image used **drive1.E01**

HashCalc and FTK Imager successfully launched

drive1.E01 successfully downloaded



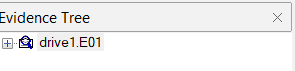
Hash Values of drive1.EO1 is as above

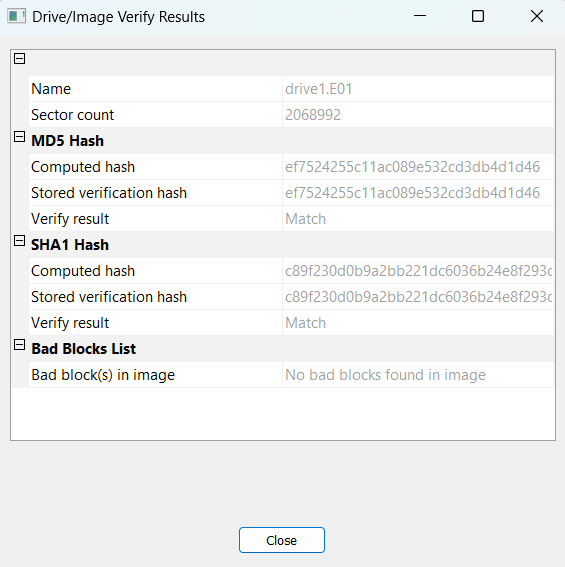
MD5 hash value is: **2ccfa510ee28712b01544594f4fad721**

SHA1 hash value is: **2baa0524e34a684e615061829b21d6b33cd906f8**

FTK Imager was successfully launched

drive1.EO1 was successfully added as evidence item in FTK Imager





Verification of the image file was as above

MD5 hash value is: **ef7524255c11ac089e532cd3db4d1d46**

SHA1 hash value is: **c89f230d0b9a2bb221dc6036b24e8f293dd0c079**

The hash values do not match

The hash values do not match because the hash values from HashCalc are for the .E01 file, which contains the data from the acquired drive, a header, CRC checks, hashes, and compression while the hash values from FTK Imager’s drive verification are only for the data from the acquired drive