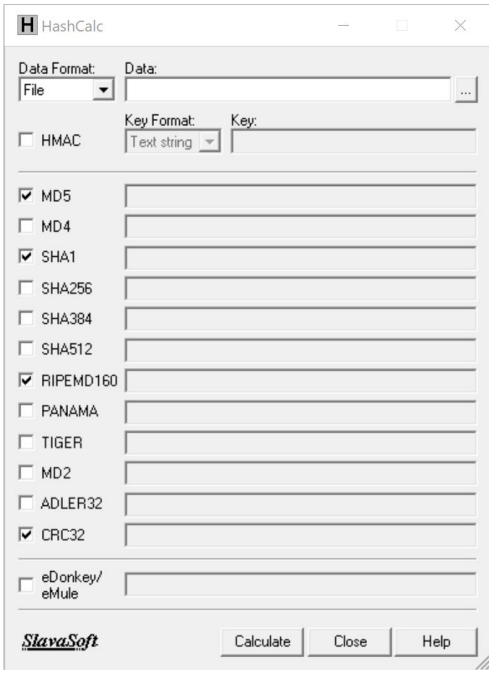
DFIR – Unit 1
Activity 1

1. Locate the text file *Tempest.txt.* Without making any changes, review the contents of this file.

2. Install and run the program HashCalc.



3. Simply drag and drop the file *Tempest.txt* into the HashCalc window.
    a. What is the MD5 Hash value of this file?

    b. What is the SHA1 Hash value of this file?

    c. What is the SHA256 hash value of this file?

4. Without changing any of the data in the text file, rename the file *Bard.txt.*

5. Using HashCalc recalculate the hash values and record them below:

a. MD5 hash value

b. SHA1 hash value

c. SHA256 hash value

6. What effect does a change of the file name have on the hash value?

7. Open the text file and do some change Save the file.

   a. What is the MD5 Hash value of this file?

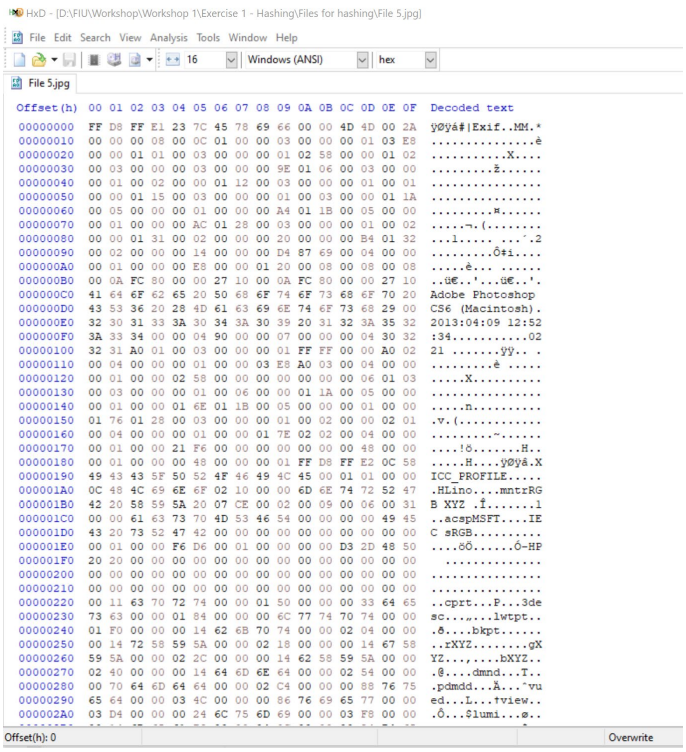
   b. What is the SHA1 Hash value of this file?

   c. What is the SHA256 hash value of this file?

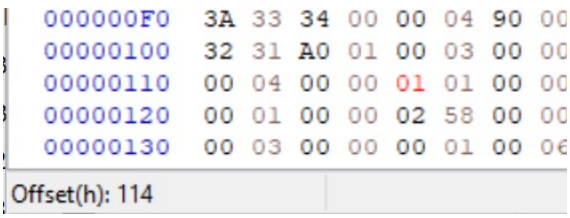
8. Calculate the Hash value of the files in the **Files for hashing** folder and record them below:

File name	MD5	SHA1
File 1.jpg		
File 2.jpg		
File 3.jpg		
File 4.jpg		
File 5.jpg		

9. Install and run the program HxD and open the file *File5.jpg*



10. Navigate to file offset (h)114 and change the value from 00 to 01 (you are changing just one bit of data – from 00000000 to 00000001)



11. Save the file as *New File 5.jpg*

12. Calculate the hash values of this new file.
    a. MD5:

    b. SHA1:

13. Using the program EPSViewer open the files *letter_of_rec.ps* and the file *order.ps* which are in the **collision** folder.

14. Briefly describe the content of these files
    a. *letter_of_rec.ps*

b. *order.ps*

15. Calculate the MD5 hash value of these two files.

File name	MD5
letter_of_rec.ps	
order.ps	

16. These two files seem to have different content but the same MD5 hash value. What is this called?

17. How might you rectify this issue?

18. The folder **USB1** contains files recovered from a suspect's thumb drive. It is believed that there may be files of value on this thumb drive. Previous examinations have identified files of value with the following MD5 hash values:

    4327397f1854d452a8a4c8dc4776738
    3
    025d7ea8904fdaa00e795286bcbe651

19. Examine the files in the **USB1** folder and identify any files that match these hash values.

20. Generate the MD5 hash value of selected files (files in Image Files Folder) using MD5 Calculator Compare the generated hash values of files with their pre-existing hash values (look into hashes.txt) to determine the integrity of files

21. Using HxD verify the filetypes given in the FileSamples Folder.

22. Examine files of various formats given in ImageFiles Folder using File Viewer and understand if they need further investigation. Also check the File Properties option to understand more on file properties.

23. Implementation of software write blocker using Thumbscrew