**LAB 1 COMPUTER FORENSIC**

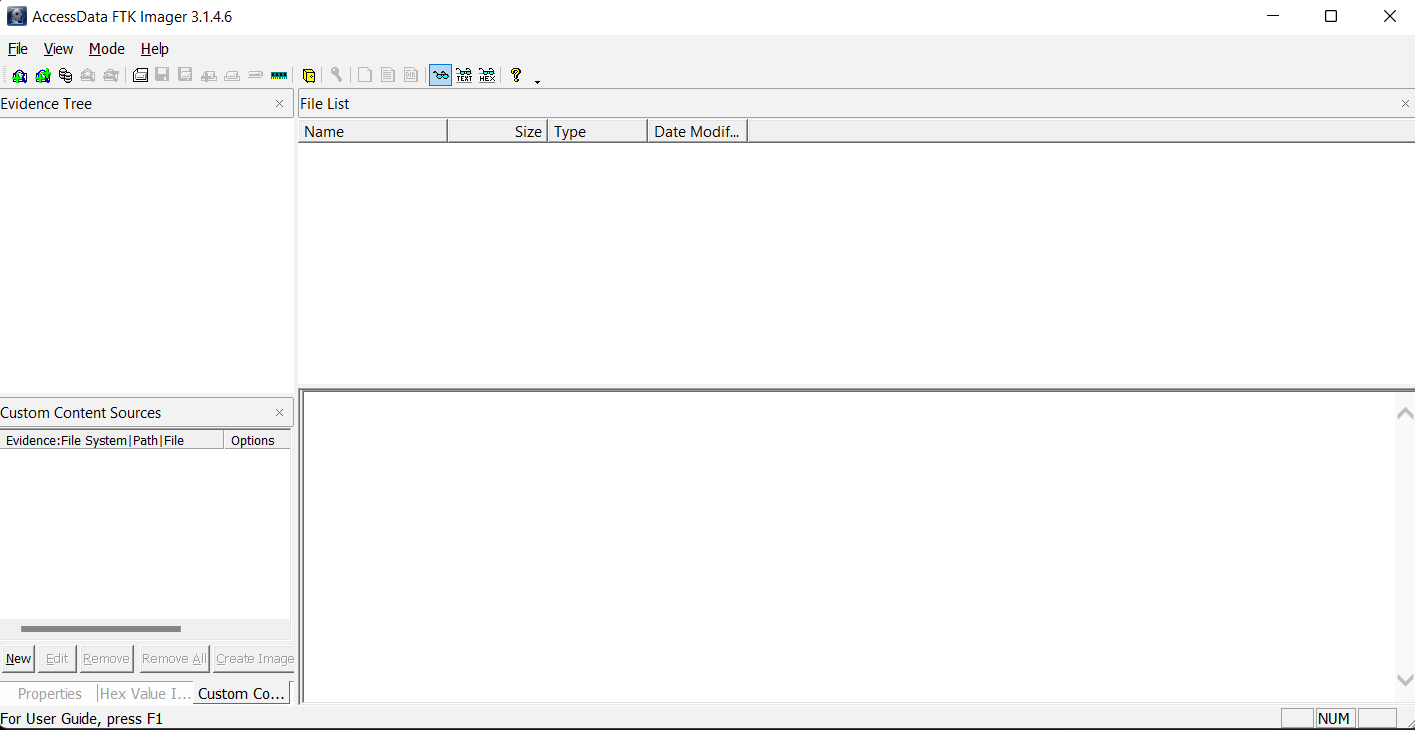
Anggota Kelompok :

1. David - 2501994506
2. Marvel Rivandy - 2502003844
3. Muhammad Mazaya Ramadhany Satrio - 2501997400
4. Ruben Pangestu - 2502010950
5. Ronan Sundjojo - 2502007382

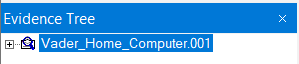
**Objectives:**

* Use HashCalc to determine the hash values of the files.
* Use HxD Hex Editor to change a single byte in a file.
* Use Hashcalc Re‐hash the files.
* Use HxD Hex Editor to examine the end of each file and determine the difference.

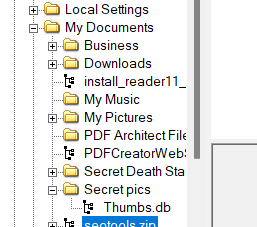
1. Open / Install Access Data’s FTK Imager 3



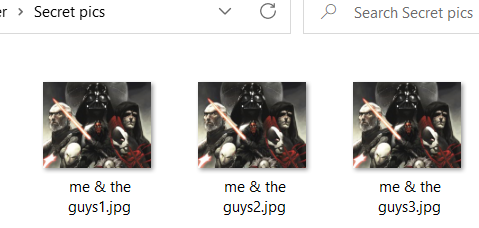
2. Select File > Add Evidence Item > Select Image File > Browse to Vader\_Home\_Computer.001 image and add it.



3. Navigate to the C:\Documents and Settings\Owner\My Documents\Secret pics folder.



4. Export the “Secret Pics” folder to your local hard drive.



5. On your computer, examine the three pictures inside the Secret pics folder. Using Windows, right click on the three provided pictures and record the size of each file.

me & the guys1.jpg size: 252 KB

me & the guys2.jpg size: 252 KB

me & the guys3.jpg size: 252 KB

6. Open each image and describe the contents.

me & the guys1.jpg Description: Picture of Sith Lords and their apprentices

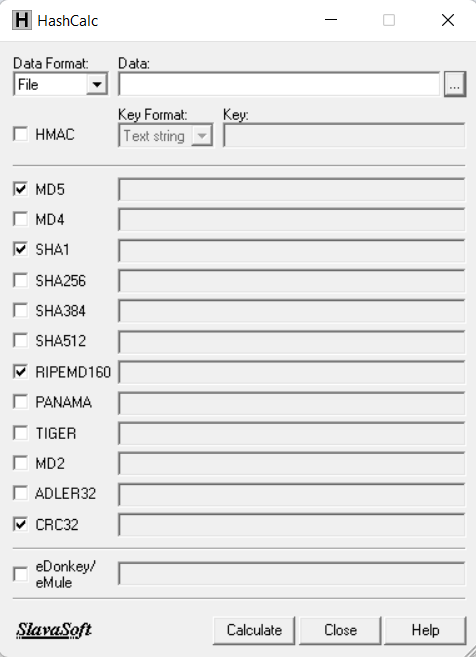
me & the guys2.jpg Description: Picture of Sith Lords and their apprentices

me & the guys3.jpg Description: Picture of Sith Lords and their apprentices

7. Are the pictures all identical?

They all look identical, except for me & the guys2.jpg which have some red pixels in the bottom right corner

8. Install Hashcalc.exe.

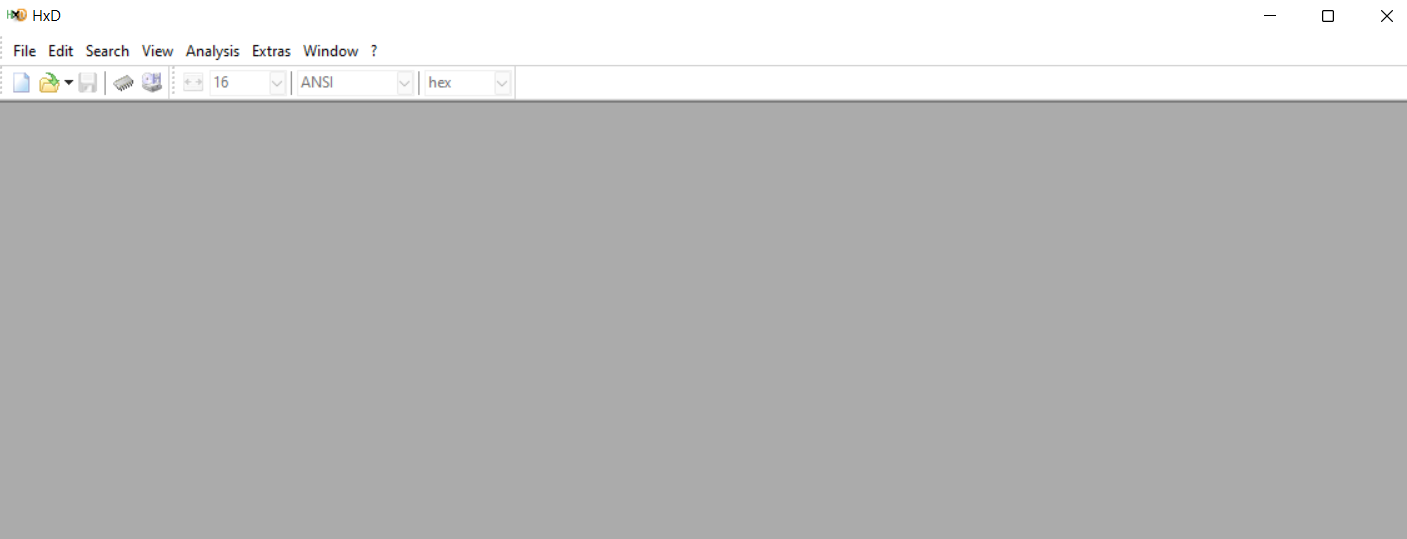


9. Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.

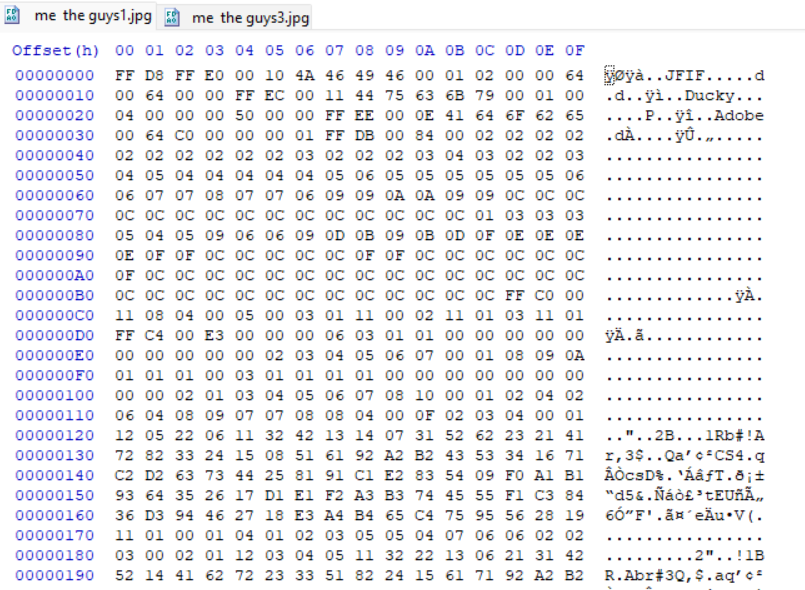
me & the guys1.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681

me & the guys2.jpg Md5 Hash: f22d2acdbb1884af86b40d72f447eca2

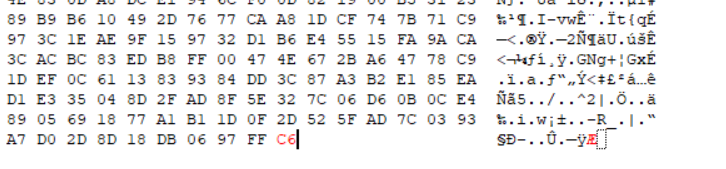
me & the guys3.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681

10. Install the HxD Hex Editor on your computer and open it. 

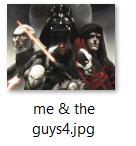
11. In HxD, select “open” under the file menu. Open one of 2 duplicate files. You know they are duplicate because they have an identical hash.



12. Go to the bottom of the file and change the last byte by selecting it and typing any character.



13. Select “Save as” under “File” and save this picture under a different name.



11. Use Windows to record the file size and hash calc for the md5 hash of the new file new file.

New File : me & the guys4.jpg

Description : Still identical to the others, Picture of Sith Lords and their apprentices

Size : 252

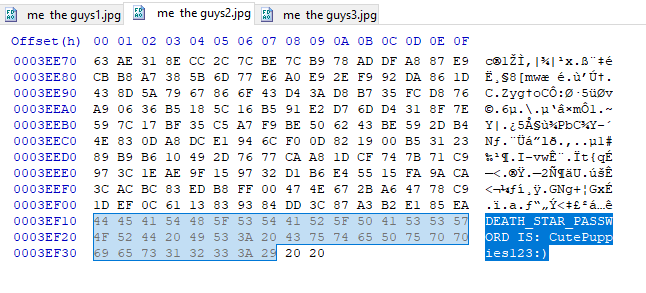
Md5 Hash : 22aa1242b9d5cf6706a5f713b14cf9dd

14. Based on the results of this test, what are your thoughts on the reliability of Md5 as a “digital fingerprint”?

Based on the results if this test, we can conclude the Md5 is reliable enough to be used as a “digital fingerprint” since it gives us different hash values for the files unless it is modified

14. Use HxD to examine the last few bytes of each of the files provided and record anything that might be of suspicion.

In me & the guys2.jpg, we can find a password



**DEATH\_STAR\_PASSWORD IS: CutePuppies123:)**

15. Based on your answer to the previous question, do you think it may be possible for criminals to effectively hide information within a jpeg file? Why?

Based on the answer, it is possible for criminals to hide information within a jpeg file, however with the right tool and the proper knowledge it is easy to uncover the hidden information