Anggota :

- AYUBI SHOLAHUDIN - 2502001441
- CARLSON KING - 2502018480
- JOSUA ABRAHAM - 2501963822
- RAMADHANA KHALAF SANDHYAKALA - 2502009412
- VAUSTIN - 2501991536

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.
    a. me & the guys1.jpg size: **251 KB (257,850 bytes) / 252 KB (258,048 bytes)**
    b. me & the guys2.jpg size: **251 KB (257,850 bytes) / 252 KB (258,048 bytes)**
    c. me & the guys3.jpg size: **251 KB (257,850 bytes) / 252 KB (258,048 bytes)**

6. Open each image and describe the contents.
    a. me & the guys1.jpg Description: **The picture of Darth Vader and The others**
    b. me & the guys2.jpg Description: **The picture of Darth Vader and The others**
    c. me & the guys3.jpg Description: **The picture of Darth Vader and The others**

7. Are the pictures all identical? **Yes**

8. Install Hashcalc.exe.

9. Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.
    a. me & the guys1.jpg Md5 Hash: **2c88e88976c4379d117854d216e36681**
    b. me & the guys2.jpg Md5 Hash: **f22d2acdbb1884af86b40d72f447eca2**
    c. 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.

Use Windows to record the file size and hash calc for the md5 hash of the new file new file.
New File:

- Description: The file type is change from JPG to FILE
- Size: **251 KB (257,850 bytes) / 252 KB (258,048 bytes)**
- Md5 Hash: **bd6a98a66e79acbccd0a134de2c1a7be**

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

- Answer :
    - As a marker whether the files we compare are the same or check whether the file is corrupt or not. Md5 is great to use, but if we look from a Security perspective Md5 may not be the best solution, because it is no longer used and is also not updated.

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

- Answer :
    - There is a CTF Flag (BRUH…) in the end of the file (me & the guys2.jpg) That saids “**DEATH_STAR_PASSWORD IS: CutePuppies123:)** “

16. 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?

- Answer :
    - Yes. Because criminals can easily place hidden files and malicious hidden texts. Inside the Hex Code of a File