Kelompok:

- 2502012363 - Calvin Winata
- 2502018316 - Darren
- 2502016771 - Elang Wisanggeni
- 2502013826 - Nicole Theresiana
- 2502039743 - Yochana Sulle

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 a nd 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: **252KB**

me & the guys2.jpg size: **252KB**

me & the guys3.jpg size: **252KB**

6. Open each image and describe the contents.

me & the guys1.jpg Description: **StarWars Villain**

me & the guys2.jpg Description: **StarWars Villain**

me & the guys3.jpg Description: **StarWars Villain**

7. Are the pictures all identical? **Yes, all of them were identical**

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 guys3 altered**

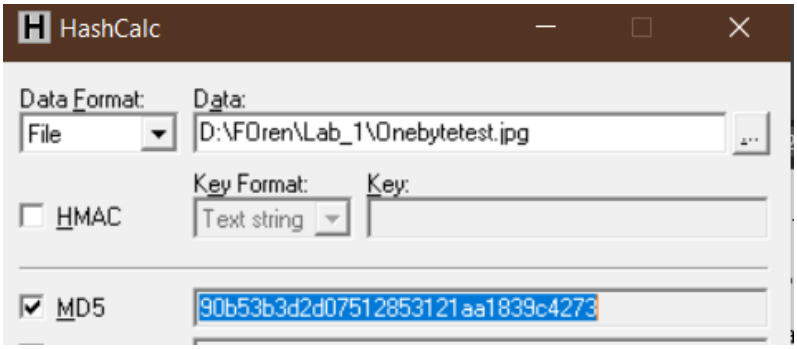
Description: **StarWars Villain**

Size: **252KB**

Md5 Hash: **6fd5b6eaa2e26505255f51c2c11d8aeb**

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

Its pretty effective to check edited or tampered data. Any changes will result in hash changes even we only change one byte of data.



This sample is a different jpg from number 11

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

By refering to the different hash that picture 2 have, we decided to check me & the guys 2. And what we find was shocking!

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?

Well it depends, its possible for them to hide information within a jpeg file. And if they have their own encryption the inspector could have a hard time trying to find the secret information hidden on the jpg. But if we are talking about readable strings / the inspector have the original picture to compare it with then its ineffective.