Kelompok:
2502064303 - Betrand Gabrialdi Leonard
2540123403 - Bertrand Redondo Mulyono (Lead)
2540123100 - Victor Benaya
2540125024 - Felysia Meytri

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: 251 KB, On Disk size: 252 KB

   me & the guys2.jpg size: 251 KB, On Disk Size: 252 KB

   me & the guys3.jpg size: 251 KB, On Disk Size: 252 KB

6. Open each image and describe the contents.

   me & the guys1.jpg Description: Sith Lords Star Wars

   me & the guys2.jpg Description: Sith Lords Star Wars

   me & the guys3.jpg Description: Sith Lords Star Wars

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.

   me & the guys1.jpg Md5 Hash: 0067808c574691536958791330b4f953

   me & the guys2.jpg Md5 Hash: 8cc6a24062d868165ed6323e717dff4c

   me & the guys3.jpg Md5 Hash: 0067808c574691536958791330b4f953

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.

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

New File: me & the boys 1.jpg

Description: For the picture is still has the same result as before, but it gives different hashing result.

Size: 251 mean while on disk still 252

Md5 Hash: 29176cd6858f837398613a0d2034970a

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

The result of a small glimpse of change makes a hugely different result. Based on the result of this test, this makes it hard for the attacker to predict the resulting hash value for modified input. Even though it has done a great job in this case, I still do not recommend it for other cases, because it has vulnerability to collision attacks, where 2 different inputs can produce the same hash value. Furthermore, MD5 algorithm is outdated so it’s very vulnerable to any cracking method.

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

For the pictures 1 and 3 it doesn't look suspicious at all. But, the 2nd picture has a suspicious message on the last byte, which is “DEATH_STAR_PASSWORD IS: CutePuppies123:)”.

17. 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?

Yes, it is possible to hide information in a jpeg file, This is called Steganography.

JPEG format type of file, can be embed some information inside the part of file where it does not change much for the picture.