2540125384 – Benedicto Marvelous Aldiajaya

2540118933 – John Orlond

2540124702 – Matthew Kurniawan

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: **Darth Vader and a lot of bad guys.**
   me & the guys2.jpg Description: **Darth Vader and a lot of bad guys with a "corrupt" pixel at the right bottom corner of the image.**
   me & the guys3.jpg Description: **Darth Vader and a lot of bad guys.**
7. Are the pictures all identical?
   No, there is a slight corruption in the right bottom corner of the me & the guys2.jpg

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.SS

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:

Description : Same picture but the right bottom corner the picture has some “Corrupt” pixel like the “me & the guys2.jpg” file.

Size:**251kb**

Md5 Hash: **d36ef2515c165726c74a2d33635baa6d**

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

Based on the test results we can conclude that the Md5 is **reliable** as a digital fingerprint. This is because the slight changes i made by changing the last byte using HxD tool, resulting a change in the Md5 hash as well. This mean that a slight alteration of an image is detected.

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

In the “me & the guys2.jpg” picture, the last byte contains an information which is **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?
    Yes it is possible, criminals can hide it using various tools and techniques. But the effectiveness depends on how well the criminal hide it.