

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 (257,850 bytes)

me & the guys2.jpg size: 251 KB (257,850 bytes)

me & the guys3.jpg size: 251 KB (257,850 bytes)

6. Open each image and describe the contents.

me & the guys1.jpg Description: 7 Star Wars Characters

me & the guys2.jpg Description: 7 Star Wars Characters

me & the guys3.jpg Description: 7 Star Wars Characters

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: 2c88e88976c4379d117854d216e36681

me & the guys2.jpg Md5 Hash: f22d2acdabb1884af86b40d72f447eca2

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: 7 Star Wars Characters

Size: 251 KB (257,850 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"?

MD5 hash dapat digunakan sebagai "digital fingerprint", karena jika seandainya terdapat chunk bytes yang berbeda, maka hasil hash pun berbeda, lain halnya dengan size berubahnya chunk bytes, tidak berpengaruh pada ukuran file, sehingga penggunaan hash lebih terpercaya

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

Pada file me & the guys2, terdapat data berupa password yaitu "DEATH_STAR_PASSWORD IS: CutePuppies123:)" pada bytes ke 0x3EF10 sampai 0x3EF37

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?

Menurut kami, ketika kriminal mencoba menyimpan informasi dengan mengubah bytes di dalam file jpeg, maka MD5 hash akan berubah, meskipun file size tidak berubah. Sehingga file yang dimodifikasi tidak akan memiliki hash yang sama dengan hash file awal.