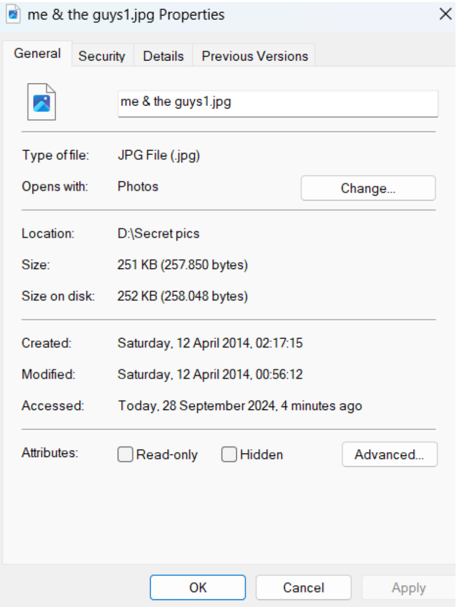
Matthew Devensen – 2602080251
Daniel Rafael Ayorbaba – 2540120723

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 Properties

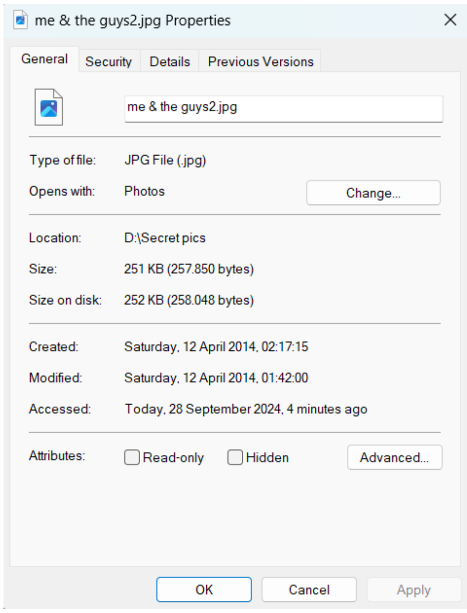
me & the guys1.jpg

Type of file: JPG File (.jpg)
Opens with: Photos

Location: D:\Secret pics
Size: 251 KB (257.850 bytes)
Size on disk: 252 KB (258.048 bytes)

Created: Saturday, 12 April 2014, 02:17:15
Modified: Saturday, 12 April 2014, 00:56:12
Accessed: Today, 28 September 2024, 4 minutes ago

Attributes: □ Read-only □ Hidden



me & the guys2.jpg Properties

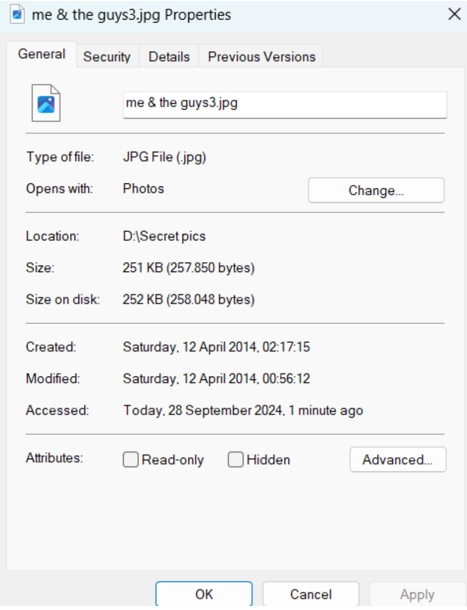
me & the guys2.jpg

Type of file: JPG File (.jpg)
Opens with: Photos

Location: D:\Secret pics
Size: 251 KB (257.850 bytes)
Size on disk: 252 KB (258.048 bytes)

Created: Saturday, 12 April 2014, 02:17:15
Modified: Saturday, 12 April 2014, 01:42:00
Accessed: Today, 28 September 2024, 4 minutes ago

Attributes: □ Read-only □ Hidden



me & the guys3.jpg

Type of file: JPG File (.jpg)

Opens with: Photos

Location: D:\Secret pics

Size: 251 KB (257.850 bytes)

Size on disk: 252 KB (258.048 bytes)

Created: Saturday, 12 April 2014, 02:17:15

Modified: Saturday, 12 April 2014, 00:56:12

Accessed: Today, 28 September 2024, 1 minute ago

Attributes: □ Read-only □ Hidden

me & the guys1.jpg size: **251 KB**

me & the guys2.jpg size: **251 KB**

me & the guys3.jpg size: **251 KB**

6. Open each image and describe the contents.

me & the guys1.jpg Description: **The image shows the enemies from Star Wars, on the left is Count Dooku, in the upper center is Darth Vader, in the upper right is Emperor Palpatine, in the middle is Darth Maul, in the lower left is Asaji Ventress, and in the lower right is Mother Talzin.**

me & the guys2.jpg Description: **The image shows the enemies from Star Wars, on the left is Count Dooku, in the upper center is Darth Vader, in the upper right is Emperor Palpatine, in the middle is Darth Maul, in the lower left is Asaji Ventress, and in the lower right is Mother Talzin.**

me & the guys3.jpg Description: **The image shows the enemies from Star Wars, on the left is Count Dooku, in the upper center is Darth Vader, in the upper right is Emperor Palpatine, in the middle is Darth Maul, in the lower left is Asaji Ventress, and in the lower right is Mother Talzin.**

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: **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:

Description: **me & the guys4.jpg**

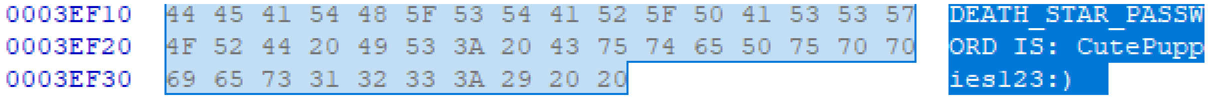
Size: **251 KB**

Md5 Hash: **efc1810da34c09457ade9f639a71034b**

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

MD5 hashing is reliable for verifying the integrity of a file because files may have the same size but contain something that cannot be seen directly.

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



```
0003EF10  44 45 41 54 48 5F 53 54 41 52 5F 50 41 53 53 57  DEATH_STAR_PASSW
0003EF20  4F 52 44 20 49 53 3A 20 43 75 74 65 50 75 70 70  ORD IS: CutePupp
0003EF30  69 65 73 31 32 33 3A 29 20 20                    ies123:)
```

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 for criminals to effectively hide information within a JPEG file, a process known as steganography. This method allows them to embed hidden data inside the image without changing the visible appearance of the file. Since files like JPEGs can have the same size and appearance, MD5 hashing can only verify file integrity but won't detect hidden data unless the hash changes. This makes it difficult to detect if information has been altered or embedded without further inspection, such as through specific steganalysis tools designed to uncover hidden data.