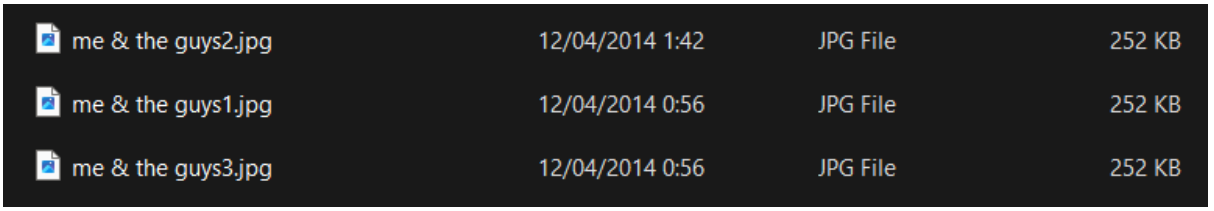
Member: (24/09/2023)
- [2540132723] Immanuel Billy Christian Santoso
- [2501998845] Jeremy Julian
- [2501983736] Johanes
- [2502008952] Richard Marchelino Wijaya Tanzil, Tan

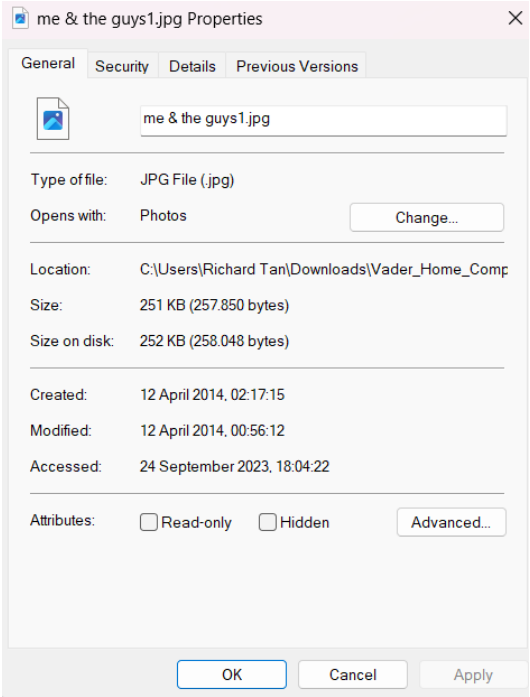
Objectives:
- Use HashCalc to determine the hash values of the files.
- Use HxD Hex Editor to change a single byte in a file.
- Use Hashcalc Re-hash the files.
- Use HxD Hex Editor to examine the end of each file and determine the difference.

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 guys2.jpg	12/04/2014 1:42	JPG File	252 KB
me & the guys1.jpg	12/04/2014 0:56	JPG File	252 KB
me & the guys3.jpg	12/04/2014 0:56	JPG File	252 KB

me & the guys1.jpg



me & the guys1.jpg Properties

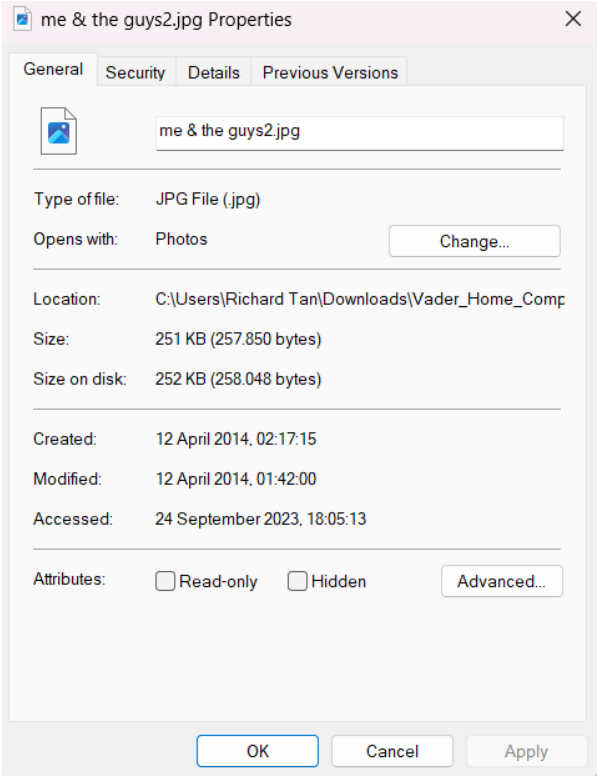
General | Security | Details | Previous Versions

me & the guys1.jpg

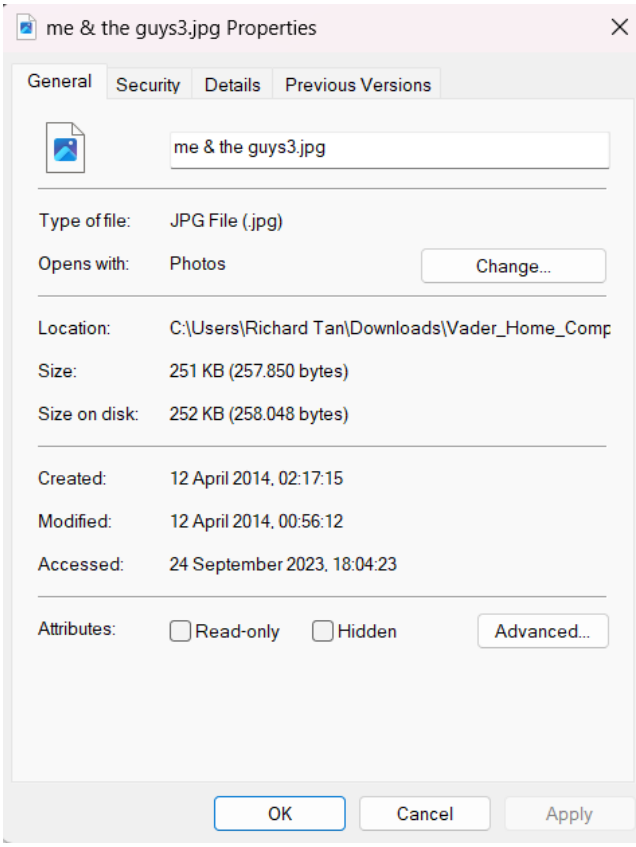
Type of file:	JPG File (.jpg)
Opens with:	Photos (Change...)
Location:	C:\Users\Richard Tan\Downloads\Vader_Home_Comp
Size:	251 KB (257.850 bytes)
Size on disk:	252 KB (258.048 bytes)
Created:	12 April 2014, 02:17:15
Modified:	12 April 2014, 00:56:12
Accessed:	24 September 2023, 18:04:22
Attributes:	Read-only, Hidden, Advanced...

OK | Cancel | Apply

me & the guys2.jpg



me & the guys3.jpg



6. **Open each image and describe the contents.**
   Me & the guys1,2 and 3 have the same image content, however, there might be a slight difference in the checksum if a hex value has been edited.

Image content	Description
	The Image contains various Darths (Sith lords), the most iconic one is Darth Vader

7. **Are the pictures all identical?**
   Image-wise, the three pictures are identical, but If we check using **sha256sum** to validate each picture we can see a slight difference here. Thus, only "**me & the guys1.jpg"** and "**me & the guys3.jpg**" are identical.

```
88c1f94bca3c647924c88c385e07f657af1095c01ecfb33927092848ef36381f  me & the guys1.jpg
9f1ddbbc43a7d81228e71c2ec4d1e7cd817596701bbd3a2b8f3b2384fa737900  me & the guys2.jpg
88c1f94bca3c647924c88c385e07f657af1095c01ecfb33927092848ef36381f  me & the guys3.jpg
```

8. **Install Hashcalc.exe.**
9. **Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file**

Image name	MD5 Hash Value
me & the guys1.jpg	2c88e88976c4379d117854d216e36681
me & the guys2.jpg	f22d2acdbb1884af86b40d72f447eca2
me & the guys3.jpg	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 duplicates 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.**

I decided to change the “**me & the guys3.jpg**” file.

me the guys3.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0003EEA0  A9 06 36 B5 18 5C 16 B5 91 E2 D7 6D D4 31 8F 7E  ©.6µ.\.µ'â×mÔ1.~
0003EEB0  59 7C 17 BF 35 C5 A7 F9 BE 50 62 43 BE 59 2D B4  Y|.¿5Å§ù¾PbC¾Y-´
0003EEC0  4E 83 0D A8 DC E1 94 6C F0 0D 82 19 00 B5 31 23  Nƒ.¨Üá”lð.‚..µ1#
0003EED0  89 B9 B6 10 49 2D 76 77 CA A8 1D CF 74 7B 71 C9  ‰¹¶.I-vwÊ¨.Ït{qÉ
0003EEE0  97 3C 1E AE 9F 15 97 32 D1 B6 E4 55 15 FA 9A CA  —<.®Ÿ.—2Ñ¶äU.úšÊ
0003EEF0  3C AC BC 83 ED B8 FF 00 47 4E 67 2B A6 47 78 C9  <¬¼ƒí¸ÿ.GNg+¦GxÉ
0003EF00  1D EF 0C 61 13 83 93 84 DD 3C 87 A3 B2 E1 85 EA  .ï.a.ƒ“„Ý<‡£²á…ê
0003EF10  D1 E3 35 04 8D 2F AD 8F 5E 32 7C 06 D6 0B 0C E4  Ñã5../..^2|.Ö..ä
0003EF20  89 05 69 18 77 A1 B1 1D 0F 2D 52 5F AD 7C 03 93  ‰.i.w¡±..-R_.|.“
0003EF30  A7 D0 2D 8D 18 DB 06 97 FF D9 6A 39 30 31 64 63  §Ð-..Û.—ÿÙj901dc
```

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.**

File name	Hexed_me & the guys3.jpg
File Properties	Location: C:\Users\Richard Tan\Downloads\Vader_Home_Comp Size: 251 KB (257.856 bytes) Size on disk: 252 KB (258.048 bytes) Created: 24 September 2023, 18:26:03 Modified: 24 September 2023, 18:26:03 Accessed: 24 September 2023, 18:26:03
File Md5 Hash	`b6fe38c8a29e9879bc9c94cc80c67a6f  hexed_me & the guys3.jpg`

File Md5 Comparison	`2c88e88976c4379d117854d216e36681  me & the guys1.jpg`
	`f22d2acdbb1884af86b40d72f447eca2  me & the guys2.jpg`
	`2c88e88976c4379d117854d216e36681  me & the guys3.jpg`
	`b6fe38c8a29e9879bc9c94cc80c67a6f  hexed_me & the guys3.jpg`

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

    Md5 is very useful to identify the integrity of a file, with just a single byte change making the Md5 value change, we can easily make sure the file we have now and the file used as evidence are exact matches or if the file has been tampered or forged.

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

Inside the hex of “**me & the guys2.jpg**” we could see there is a message saying “DEATH_START_PASSWORD IS: CutePuppies123;)”

me the guys2.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

0003EE70  63 AE 31 8E CC 2C 7C BE 7C B9 78 AD DF A8 87 E9  c®1ŽÌ,|¾|¹x.ß¨‡é
0003EE80  CB B8 A7 38 5B 6D 77 E6 A0 E9 2E F9 92 DA 86 1D  Ë¸§8[mwæ é.ù’Ú†.
0003EE90  43 8D 5A 79 67 86 6F 43 D4 3A D8 B7 35 FC D8 76  C.ZygtoCÔ:Ø·5üØv
0003EEA0  A9 06 36 B5 18 5C 16 B5 91 E2 D7 6D D4 31 8F 7E  ©.6µ.\.µ‘â×mÔ1.~
0003EEB0  59 7C 17 BF 35 C5 A7 F9 BE 50 62 43 BE 59 2D B4  Y|.¿5Å§ù¾PbC¾Y-´
0003EEC0  4E 83 0D A8 DC E1 94 6C F0 0D 82 19 00 B5 31 23  Nƒ.¨Üá”lð.,..µ1#
0003EED0  89 B9 B6 10 49 2D 76 77 CA A8 1D CF 74 7B 71 C9  ‰¹¶.I-vwÊ¨.Ït{qÉ
0003EEE0  97 3C 1E AE 9F 15 97 32 D1 B6 E4 55 15 FA 9A CA  —<.®Ÿ.—2Ñ¶äU.úšÊ
0003EEF0  3C AC BC 83 ED B8 FF 00 47 4E 67 2B A6 47 78 C9  <¬¼ƒí¸ÿ.GNg+¦GxÉ
0003EF00  1D EF 0C 61 13 83 93 84 DD 3C 87 A3 B2 E1 85 EA  .ï.a.ƒ“„Ý<‡£²á…ê
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:)
```

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. A criminal can hide various types of data ranging from just a simple message/text like the previous answer, or even using the jpeg to hide a reverse shell or even malware that can harm the victim's devices.