LAB 1 COMPUTER FORENSIC

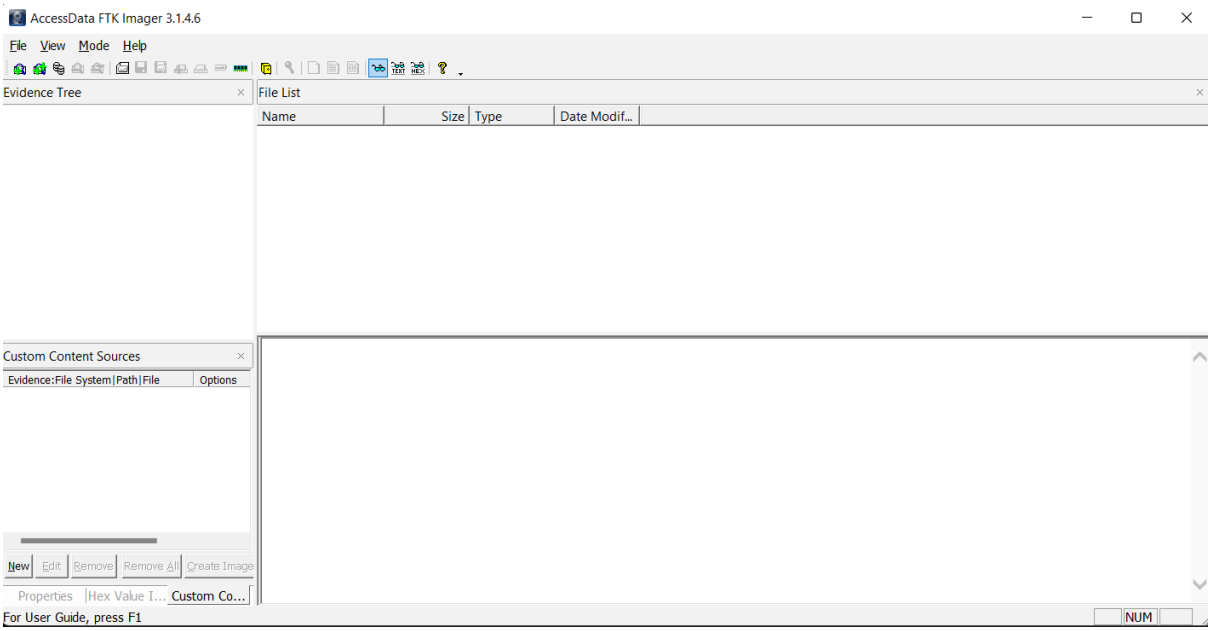
Anggota Kelompok :

1. David - 2501994506
2. Marvel Rivandy - 2502003844
3. Muhammad Mazaya Ramadhany Satrio - 2501997400
4. Ruben Pangestu - 2502010950
5. Ronan Sundjojo - 2502007382

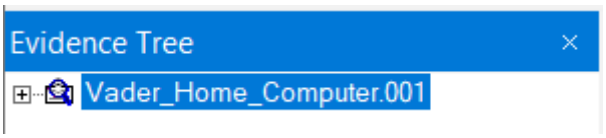
Objectives:

- 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.

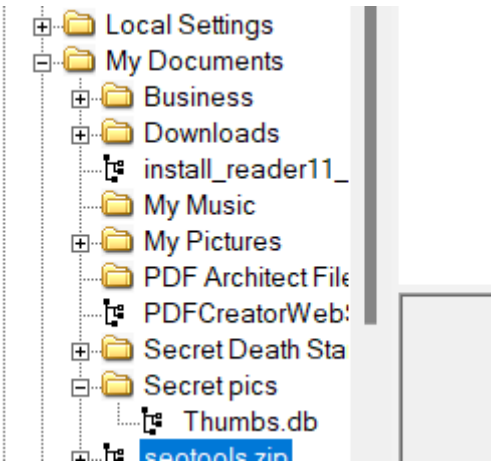
1. Open / Install Access Data's FTK Imager 3



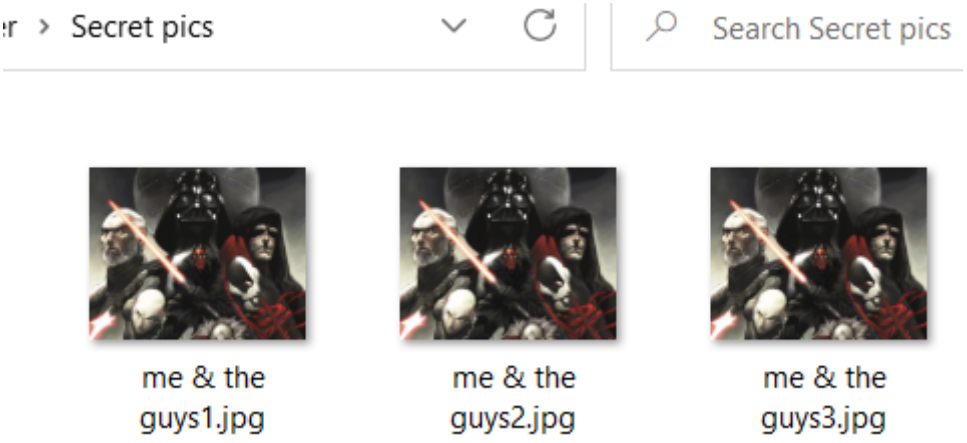
2. Select File > Add Evidence Item > Select Image File > Browse to Vader_Home_Computer.001 image and add it.



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: Picture of Sith Lords and their apprentices

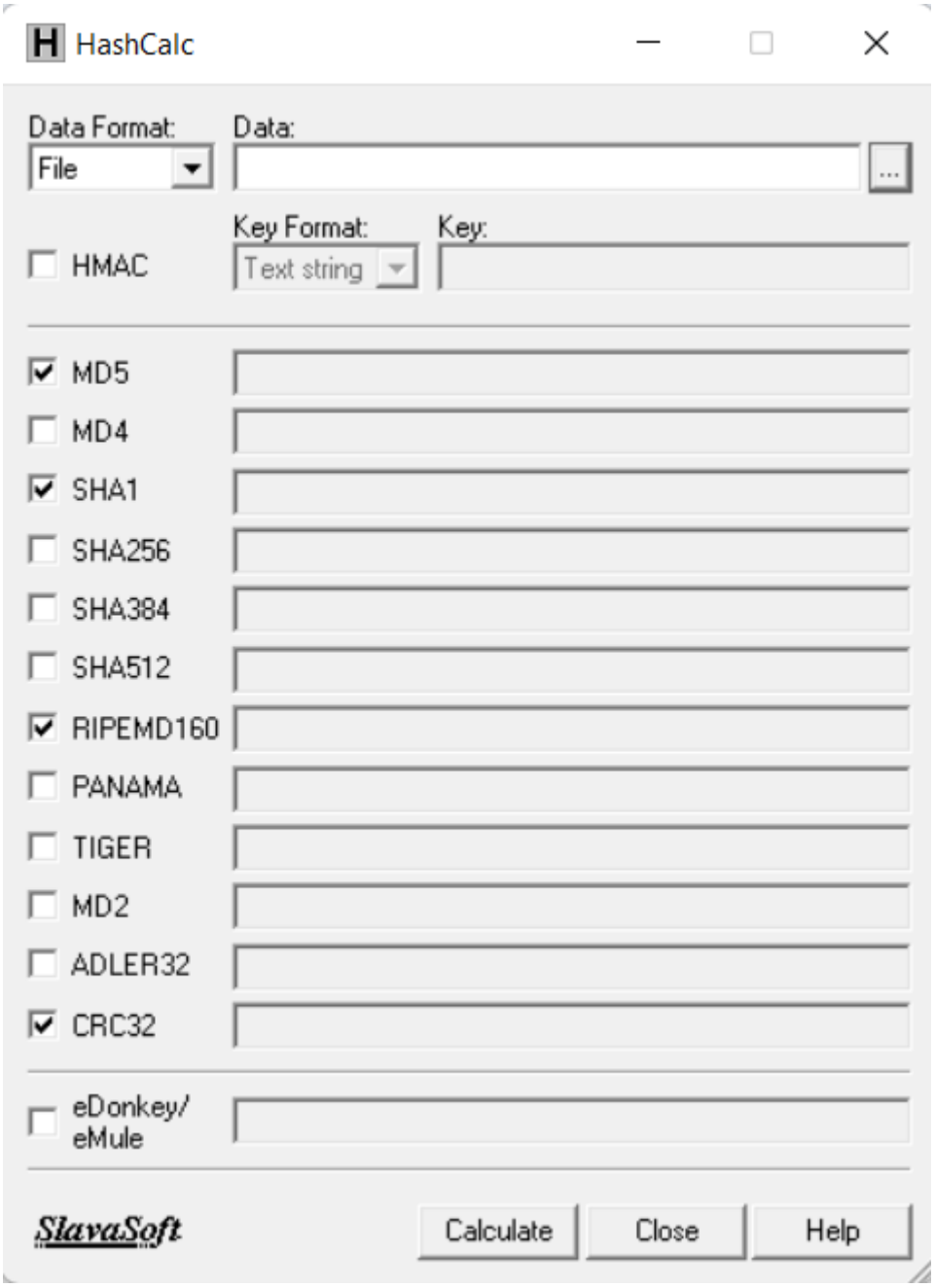
me & the guys2.jpg Description: Picture of Sith Lords and their apprentices

me & the guys3.jpg Description: Picture of Sith Lords and their apprentices

7. Are the pictures all identical?

They all look identical, except for me & the guys2.jpg which have some red pixels in the bottom right corner

8. Install Hashcalc.exe.



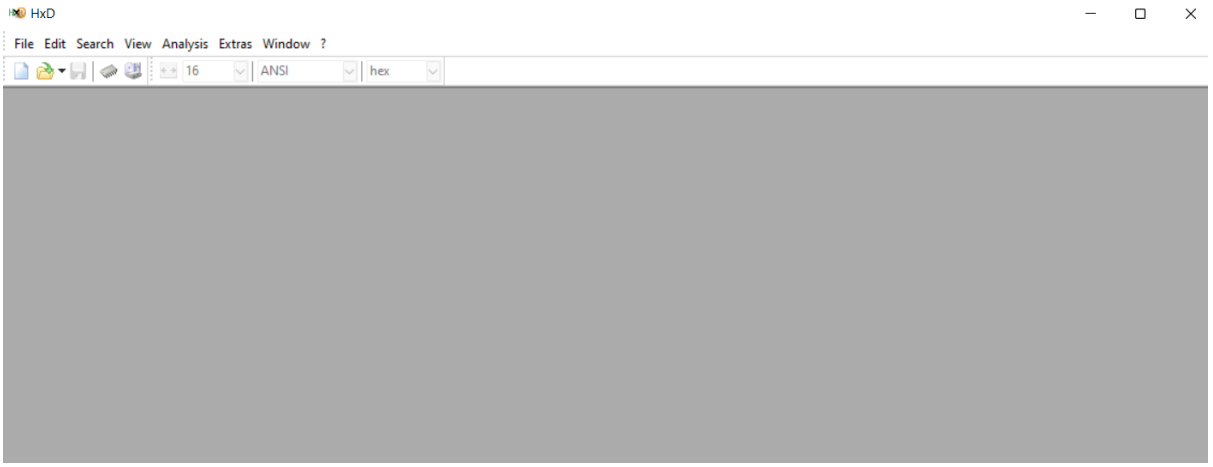
9. Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.

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.

me the guys1.jpg me the guys3.jpg

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	00	00	64	ÿØÿà..JFIF.....d
00000010	00	64	00	00	FF	EC	00	11	44	75	63	6B	79	00	01	00	.d..ÿì..Ducky...
00000020	04	00	00	00	50	00	00	FF	EE	00	0E	41	64	6F	62	65	....P..ÿî..Adobe
00000030	00	64	C0	00	00	00	01	FF	DB	00	84	00	02	02	02	02	.dÀ....ÿÛ.„.....
00000040	02	02	02	02	02	02	03	02	02	02	03	04	03	02	02	03	.....
00000050	04	05	04	04	04	04	04	05	06	05	05	05	05	05	05	06	.....
00000060	06	07	07	08	07	07	06	09	09	0A	0A	09	09	0C	0C	0C	.....
00000070	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	01	03	03	03	.....
00000080	05	04	05	09	06	06	09	0D	0B	09	0B	0D	0F	0E	0E	0E	.....
00000090	0E	0F	0F	0C	0C	0C	0C	0C	0F	0F	0C	0C	0C	0C	0C	0C	.....
000000A0	0F	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	.....
000000B0	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	0C	FF	C0	00	.....ÿÀ.
000000C0	11	08	04	00	05	00	03	01	11	00	02	11	01	03	11	01	.....
000000D0	FF	C4	00	E3	00	00	00	06	03	01	01	00	00	00	00	00	ÿÄ.ã.....
000000E0	00	00	00	00	00	02	03	04	05	06	07	00	01	08	09	0A	.....
000000F0	01	01	01	00	03	01	01	01	01	00	00	00	00	00	00	00	.....
00000100	00	00	02	01	03	04	05	06	07	08	10	00	01	02	04	02	.....
00000110	06	04	08	09	07	07	08	08	04	00	0F	02	03	04	00	01	.....
00000120	12	05	22	06	11	32	42	13	14	07	31	52	62	23	21	41	..".2B...1Rb#!A
00000130	72	82	33	24	15	08	51	61	92	A2	B2	43	53	34	16	71	r,3$..Qa’¢²CS4.q
00000140	C2	D2	63	73	44	25	81	91	C1	E2	83	54	09	F0	A1	B1	ÂÒcsD%.‘ÁâƒT.ð¡±
00000150	93	64	35	26	17	D1	E1	F2	A3	B3	74	45	55	F1	C3	84	“d5&.ÑáòÂ£³tEUñÃ„
00000160	36	D3	94	46	27	18	E3	A4	B4	65	C4	75	95	56	28	19	6Ó”F'.ã¤´eÄu•V(.
00000170	11	01	00	01	04	01	02	03	05	05	04	07	06	06	02	02	.....
00000180	03	00	02	01	12	03	04	05	11	32	22	13	06	21	31	42	.....2"..!1B
00000190	52	14	41	62	72	23	33	51	82	24	15	61	71	92	A2	B2	R.Abr#3Q,$.aq’¢²

12. Go to the bottom of the file and change the last byte by selecting it and typing any character.

```
89 B9 B6 10 49 2D 76 77 CA A8 1D CF 74 7B 71 C9  ‰¹¶.I-vwÊ¨.Ït{qÉ
97 3C 1E AE 9F 15 97 32 D1 B6 E4 55 15 FA 9A CA  —<.®Ÿ.—2Ñ¶äU.úšÊ
3C AC BC 83 ED B8 FF 00 47 4E 67 2B A6 47 78 C9  <¬¼ƒí¸ÿ.GNg+¦GxÉ
1D EF 0C 61 13 83 93 84 DD 3C 87 A3 B2 E1 85 EA  .ï.a.ƒ"„Ý<‡£²á…ê
D1 E3 35 04 8D 2F AD 8F 5E 32 7C 06 D6 0B 0C E4  Ñã5../..^2|.Ö..ä
89 05 69 18 77 A1 B1 1D 0F 2D 52 5F AD 7C 03 93  ‰.i.w¡±..-R_.|."
A7 D0 2D 8D 18 DB 06 97 FF C6                    §Ð-..Û.—ÿÆ
```

13. Select “Save as” under “File” and save this picture under a different name.

me & the guys4.jpg

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 : Still identical to the others, Picture of Sith Lords and their apprentices

Size : 252

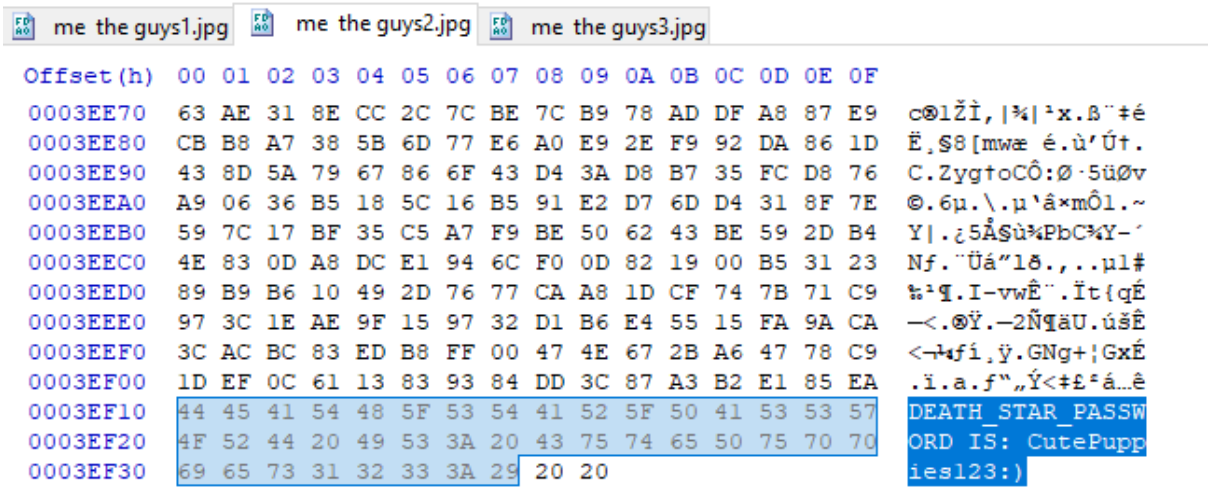
Md5 Hash : 22aa1242b9d5cf6706a5f713b14cf9dd

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

Based on the results if this test, we can conclude the Md5 is reliable enough to be used as a “digital fingerprint” since it gives us different hash values for the files unless it is modified

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

In me & the guys2.jpg, we can find a password



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?

Based on the answer, it is possible for criminals to hide information within a jpeg file, however with the right tool and the proper knowledge it is easy to uncover the hidden information