

LAB 1 Computer Forensics

Kelompok:

2501981270 - AGUSTINUS LEONARDO DWITAMA

2501989550 - MUHAMAD DWI APRIYANTO

2502001864 - RAVI DEEVAN SATYAKI

2501965052 - KEVIN MORRIS ARMANDO

2501983723 - NATANAEL FRANSISCO

Objectives:

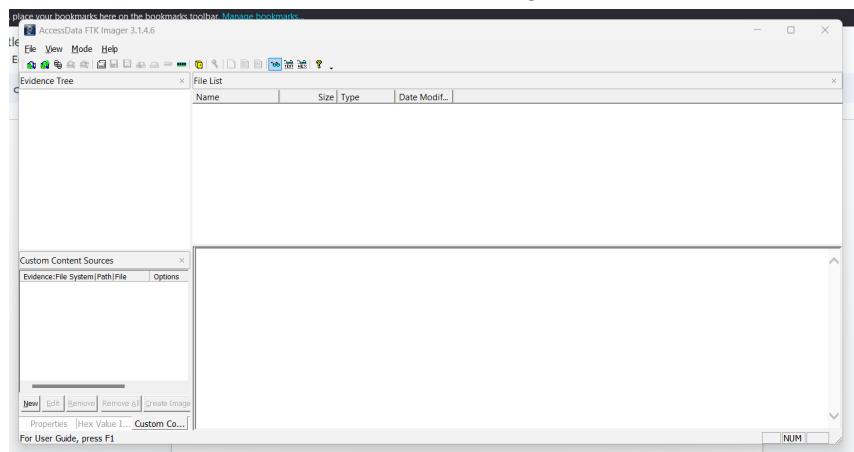
Use HashCalc to determine the hash values of the files.

Use HxD Hex Editor to change a single byte in a file.

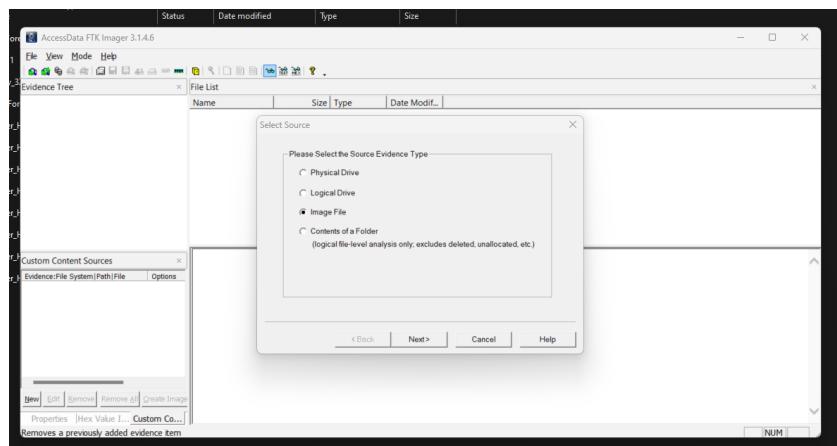
Use Hashcalc Re-hash the files.

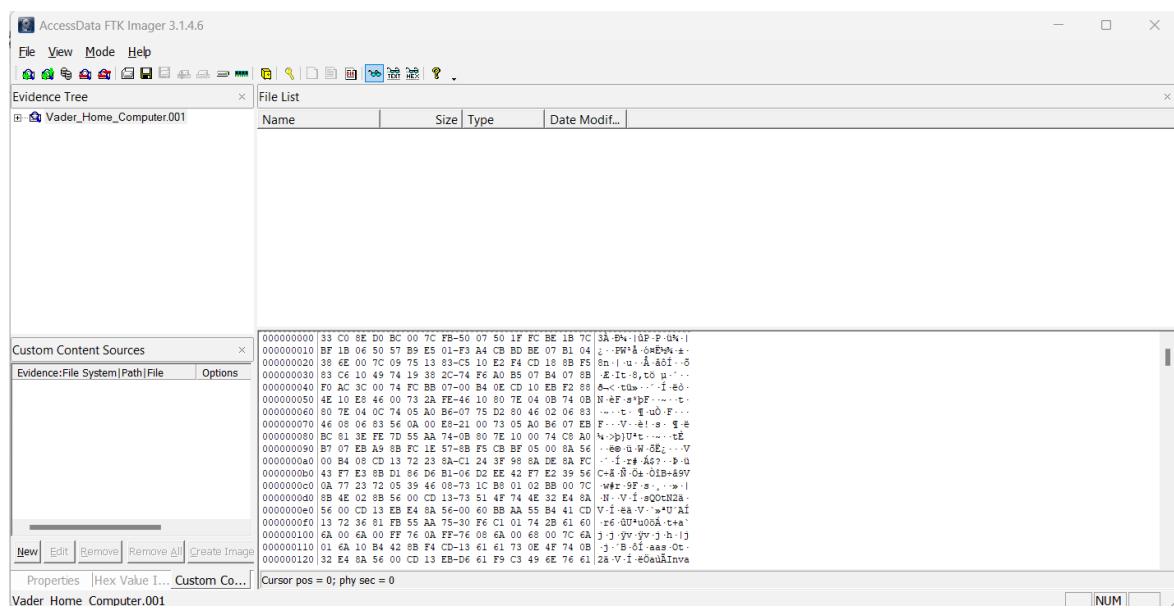
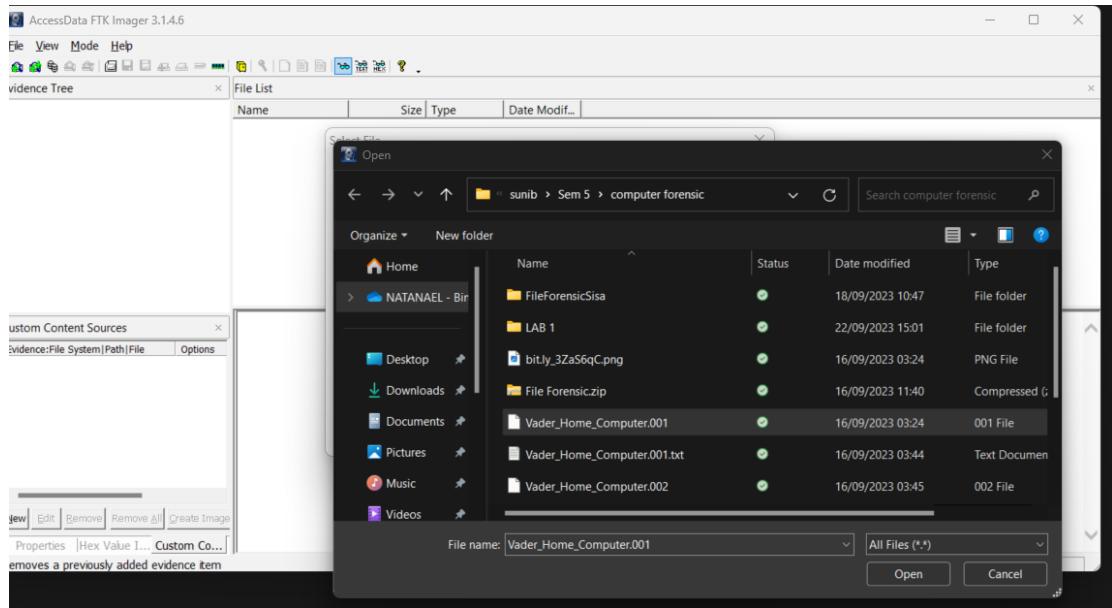
Use HxD Hex Editor to examine the end of each file and determine the difference.

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.

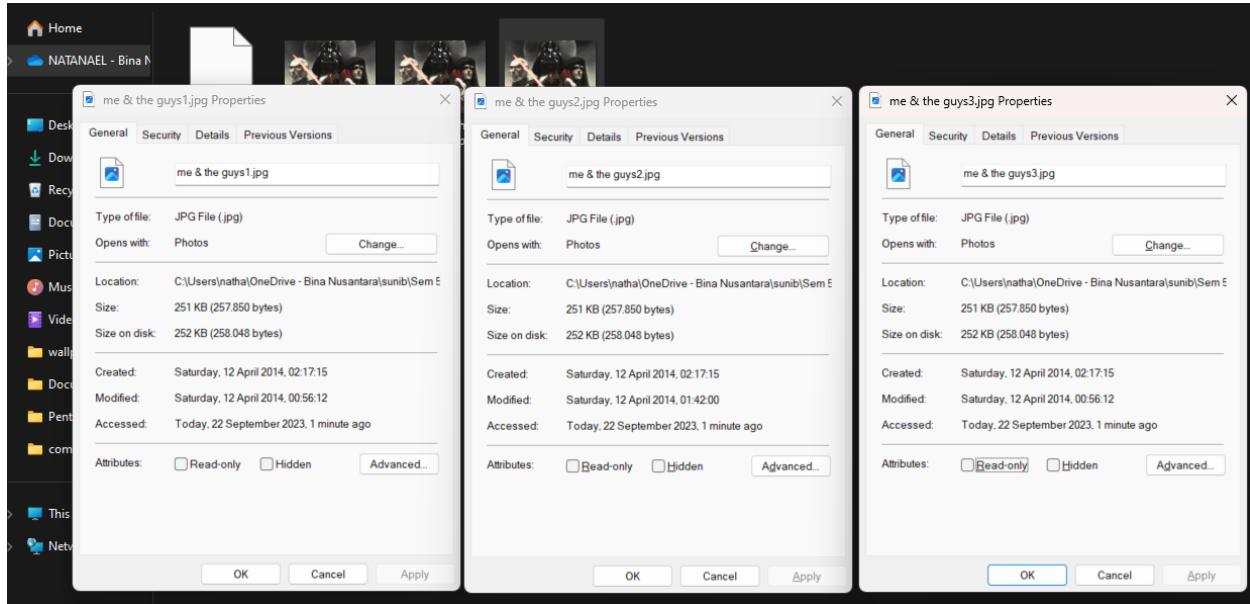
4. Export the “Secret Pics” folder to your local hard drive.

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: gambar berupa 4 tokoh antagonist dari seri star wars yang cocok dengan nama dari image yaitu *vader's home computer* karena merupakan nama salah satu antagonisnya yang ada di gambar tetapi tidak ada yang aneh tentang gambar.



me & the guys2.jpg Description: gambar kedua adalah gambar yang sama dengan yang gambar 1 hanya saja terdapat seperti pergeseran dari gambar pertama.

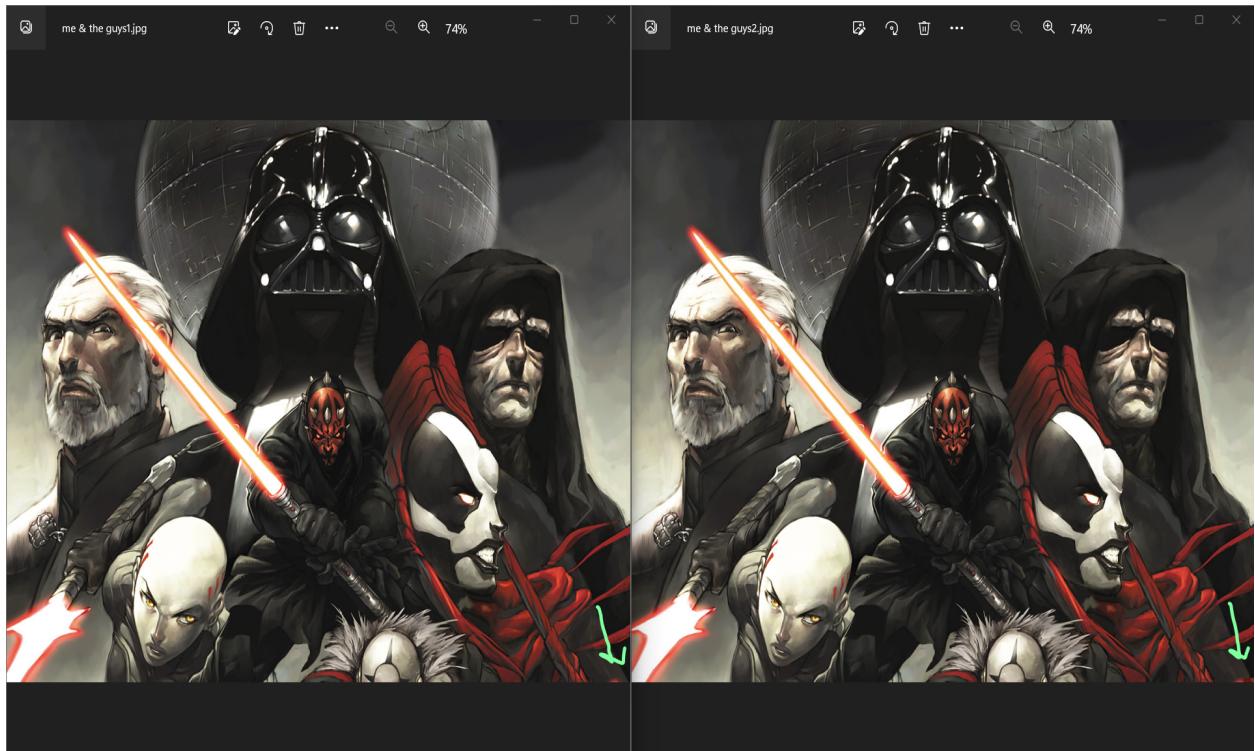


me & the guys3.jpg Description: kalo dilihat yang ketiga juga adalah gambar yang sama tetapi kalo dilihat sama seperti gambar 1 dan tidak ada hal yang aneh.

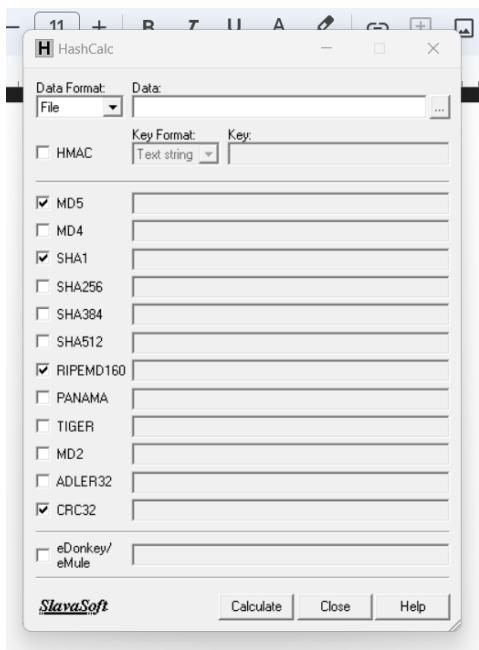


7. Are the pictures all identical?

Sepertinya tidak gambar 1 dan 3 terlihat mirip tetapi gambar 2 ada kejanggalan di pojok kanan bawah.



8. Install Hashcalc.exe.

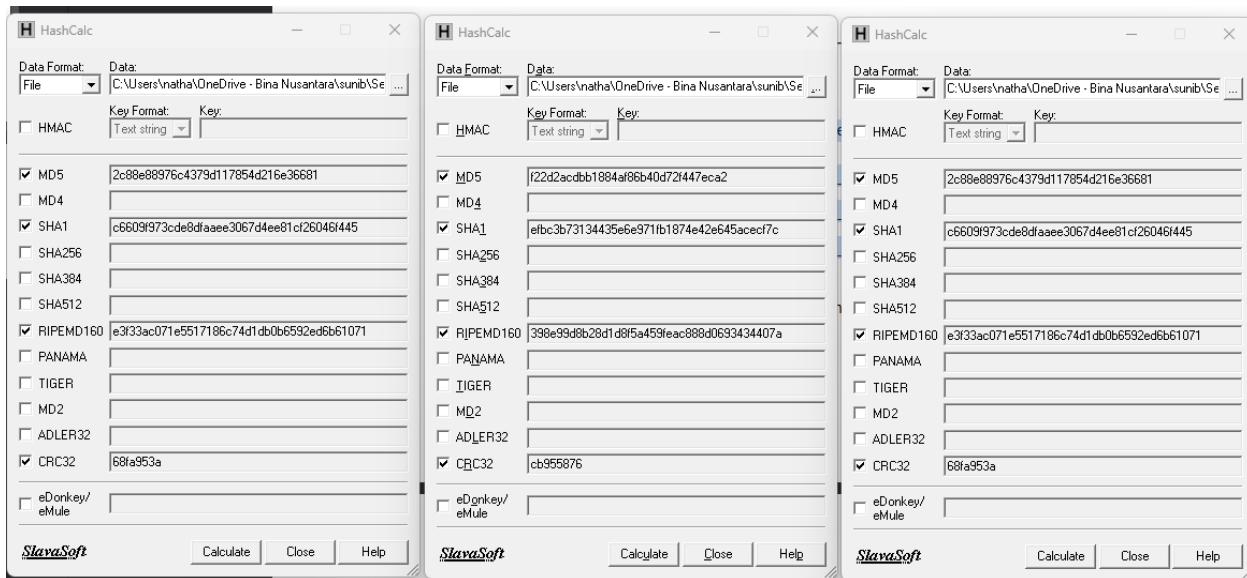


9. Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.

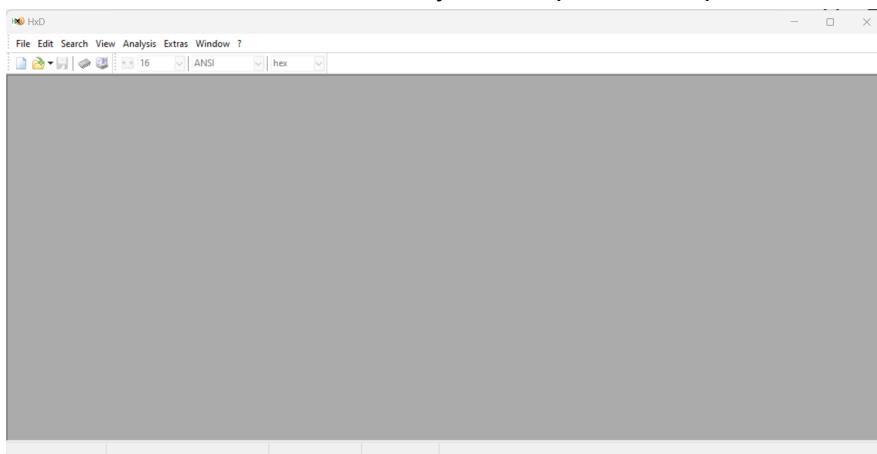
me & the guys1.jpg Md5 Hash: **2c88e88976c4379d117854d216e36681**

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.

HxD - [C:\Users\natha\OneDrive - Bina Nusantara\sunib\Sem 5\computer forensic\LAB 1\Secret pics\me & the guys1.jpg]

File Edit Search View Analysis Extras Window ?

me the guys1.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 J\b\j\à..JFIF...d
00000010 00 64 00 00 FF EC 00 11 44 75 63 6B 79 00 01 00 .d..y\ì..Ducky...
00000020 04 00 00 50 00 FF EE 00 0E 41 64 6F 62 65 ...P..y\ì..Adobe
00000030 00 64 C0 00 00 00 01 FF DB 00 84 00 02 02 02 .dA...y\ì...
00000040 02 02 02 02 02 02 03 02 02 03 03 02 02 03 ..... .
00000050 04 05 04 04 04 04 04 05 06 05 05 05 05 05 06 ..... .
00000060 06 07 07 07 07 07 06 09 0A 09 09 09 0C 0C 0C ..... .
00000070 0C 01 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 ..... .
000000B0 OC 0C FF C0 00 ..... y\ì.
000000C0 11 08 04 00 05 00 03 01 11 00 02 11 01 03 11 01 ..... .
000000D0 FF C4 00 E3 00 00 06 03 01 01 00 00 00 00 00 00 y\ì..A..... .
000000E0 00 00 00 00 02 03 04 05 06 07 00 01 08 09 0A ..... .
000000F0 01 01 00 03 01 01 01 00 00 00 00 00 00 00 00 00 ..... .
00000100 00 00 02 03 04 05 06 07 08 10 00 01 02 04 02 ..... .
00000110 00 04 08 08 07 07 08 08 04 00 0F 02 03 04 00 01 ..... ,.2B...1Rb#!A
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,35..Qe'c^CS4.q
00000140 C2 D2 63 73 44 25 81 91 C1 E2 83 54 09 F0 A1 B1 ÁccsDt..Á&T.T.ß±
00000150 93 64 35 26 17 D1 E1 F2 A3 B3 74 45 55 F1 C3 84 "d5s..Náöé'tEUñá.
00000160 36 D3 94 46 27 18 E3 A4 B4 65 C4 75 95 56 28 19 60"r..ß&eñu'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 S2 14 41 62 72 23 33 51 62 24 15 61 71 92 A2 B2 R.Abr#3Q,S.aq'c^
```

Offset: 0 Overwrite

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

HxD - [C:\Users\natha\OneDrive - Bina Nusantara\sunib\Sem 5\computer forensic\LAB 1\coba\me & the guys1.jpg]

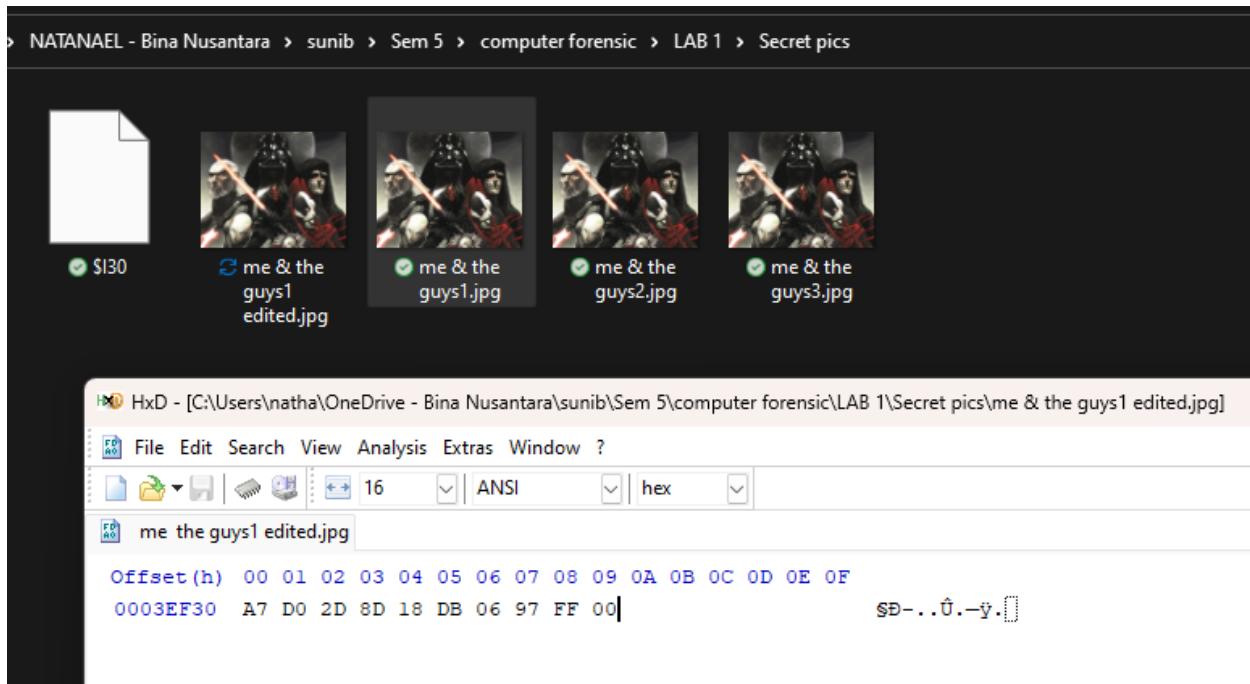
File Edit Search View Analysis Extras Window ?

me the guys1.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 0F 7E ©.éu.\.µ'â×môl.~
0003EEB0 59 7C 17 BF 35 C5 A7 F9 BE 50 62 43 BE 59 2D B4 Yl..éSôùMôPbCMY-
0003EEC0 4E 83 0D A8 DC E1 94 6C F0 0D 82 19 00 B5 31 23 Nf..Üá"18.,..µl#
0003EED0 89 B9 B6 10 49 2D 76 77 CA A8 1D CF 74 7B 71 C9 ¶.¶.I.-vwÉ'.Ít(qÈ
0003EEE0 97 3C 1E AE 9F 15 97 32 D1 B6 E4 55 15 FA 9A CA --<.ØY.-2ÑqáU.úšÈ
0003EEF0 3C AC BC 83 ED BB FF 00 47 4E 67 2B A6 47 78 C9 <-+fi..ý.GNg+!GxÈ
0003EF00 1D EF 0C 61 13 83 93 84 DD 3C 87 A3 B2 E1 85 EA ..i.a.f",Ý<#ë*á..è
0003EF10 D1 E3 35 04 8D 2F AD 8F 5E 32 7C 06 D6 0B OC E4 Ñá5//..^2|..O..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 00 $D-..Û.-y.[]
```

Offset: 3EF3A * Modified * Overwrite

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: me & the guys1 edited.jpg

Description: Secara gambar 1 dan 1 yang saya edit tidak ada terlihat perubahan visual

Size: 251 KB (257.850 bytes)

Md5 Hash: 85dc38d8c638a00bbf969e7cc2f30eca

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

Menurut saya md5 termasuk reliable untuk mengidentifikasi integritas suatu file, untuk mengetahui apakah ada suatu modifikasi yang terjadi pada file tersebut. Karena dalam kasus ini sifatnya melekat pada integritas file. Seharusnya kekurangan md5 yang mudah untuk terjadi collision tidak terlalu berpengaruh pada reliabilitas.

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

HxD - [C:\Users\natha\OneDrive - Bina Nusantara\sunib\Sem 5\computer forensic\LAB 1\Secret pics\me & the guys2.jpg]

File Edit Search View Analysis Extras Window ?

me the guys1 edited.jpg me the guys1.jpg me the guys2.jpg me the guys3.jpg

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0003EE40	17 2E 29 FC A9 85 8D E2 DE C9 66 49 2D 47 12 CC ..)ü@...âþÉfI-G.i
0003EE50	01 68 E2 D9 8F 8D F5 1C 2E 5B F4 B1 7E 14 6D C2 .hâÜ..ö..[ô±~.må
0003EE60	8F 32 BD DB F1 0B 0A CD 91 E0 BF 33 EB A5 D6 F3 .2¾Ûñ..Í'àç3ë¥Öö
0003EE70	63 AE 31 8E CC 2C 7C BE 7C B9 78 AD DF A8 87 E9 c@lžì, % ^x.B"‡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 @.6u.\.u'â*xmÔl.~
0003EEB0	59 7C 17 BF 35 C5 A7 F9 BE 50 62 43 BE 59 2D B4 Y .ç5Å\$ù%PbC%Y-`
0003EEC0	4E 83 0D A8 DC E1 94 6C F0 0D 82 19 00 B5 31 23 Nf."Üá"18...µl#
0003EED0	89 B9 B6 10 49 2D 76 77 CA A8 1D CF 74 7B 71 C9 %`¶.I-vwÈ".Ít{qÈ
0003EEE0	97 3C 1E AE 9F 15 97 32 D1 B6 E4 55 15 FA 9A CA —<.ØÝ.-2Ñ¶äU.úšÈ
0003EEF0	3C AC BC 83 ED B8 FF 00 47 4E 67 2B A6 47 78 C9 <-+fi,ý.GNg+;GxE
0003EF00	1D EF OC 61 13 83 93 84 DD 3C 87 A3 B2 E1 85 EA .i.a.f",Ý<‡£"á...ê
0003EF10	44 45 41 54 48 5F 53 54 41 52 5F 50 41 53 53 57 DEATH_STAR_PASSWORD IS: CutePupp
0003EF20	4F 52 44 20 49 53 3A 20 43 75 74 65 50 75 70 70 ies123:)
0003EF30	69 65 73 31 32 33 3A 29 20 20

DEATH_STAR_PASSWORD IS: CutePuppies123:)

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?

Menurut saya possible tetapi untuk efektivitas sepertinya tergantung, karena dilihat dari gambar no.16 terlihat bahwa di dalam gambar tersebut pada byte nya disisipkan informasi penting berupa password. Bila kita kurang jelih kita tidak dapat melihat kejanggalan pada gambar tetapi dengan sedikit membongkar hash dan hex nya kita menemukan perbedaan.