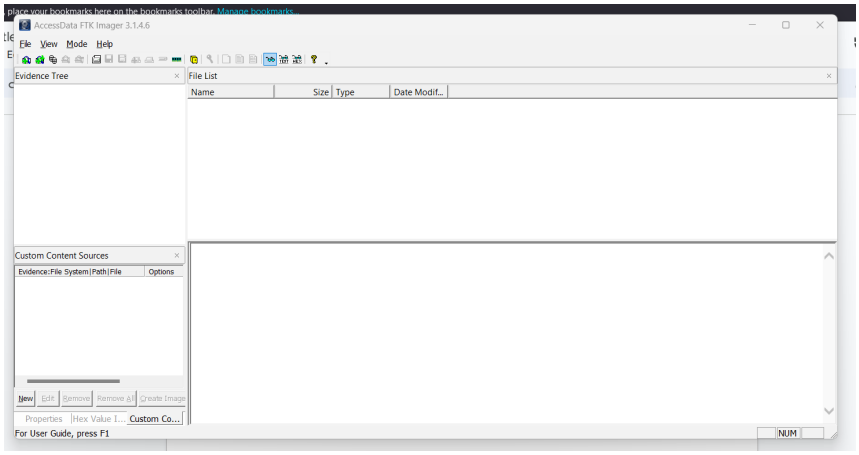
LAB 1 Computer Forensics

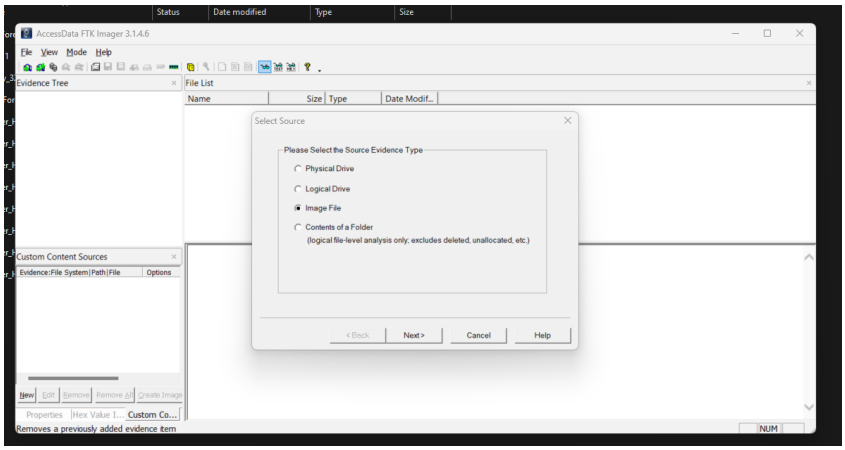
Kelompok:
2501981270 - AGUSTINUS LEONARDO DWITAMA
2501989550 - MUHAMAD DWI APRIYANTO
2502001864 - RAVI DEEVAN SATYAKI
2501965052 - KEVIN MORRIS ARMANDO
2501983723 - NATANAEL FRANSISCO

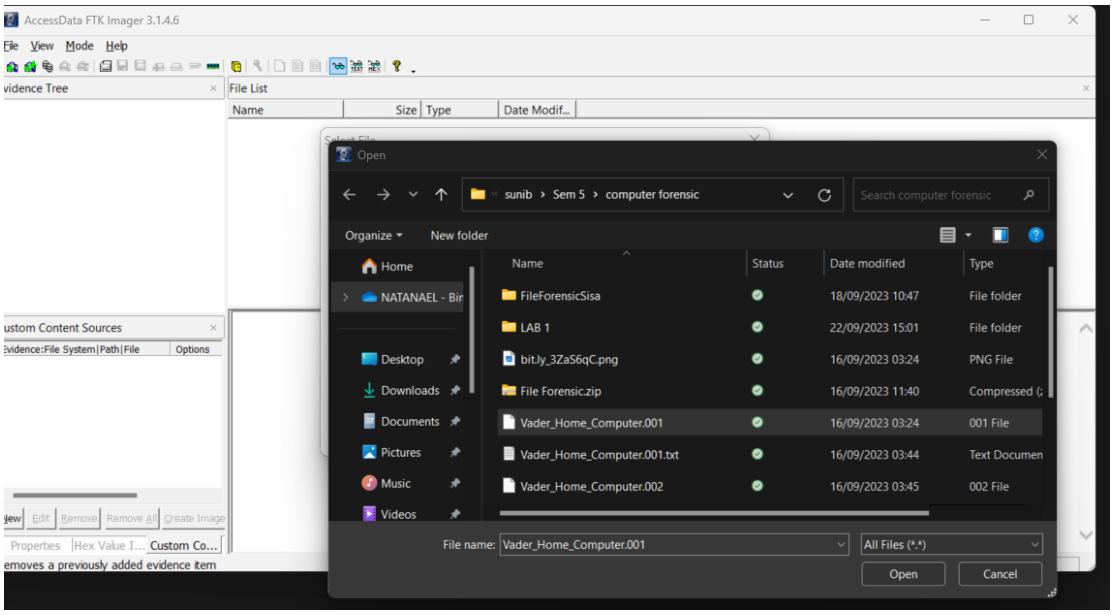
Objectives:
Use HashCalc to determine the hash values of the files.
Use HxD Hex Editor to change a single byte in a file.
Use Hashcalc Re-hash the files.
Use HxD Hex Editor to examine the end of each file and determine the difference.

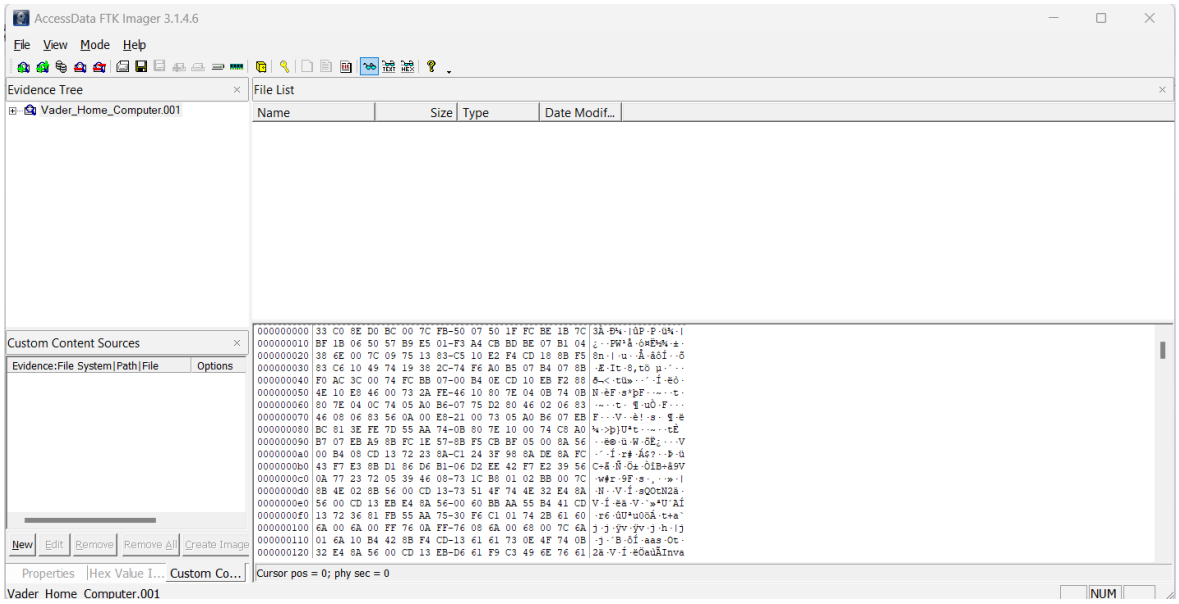
1. Open / Install Access Data's FTK Imager 3



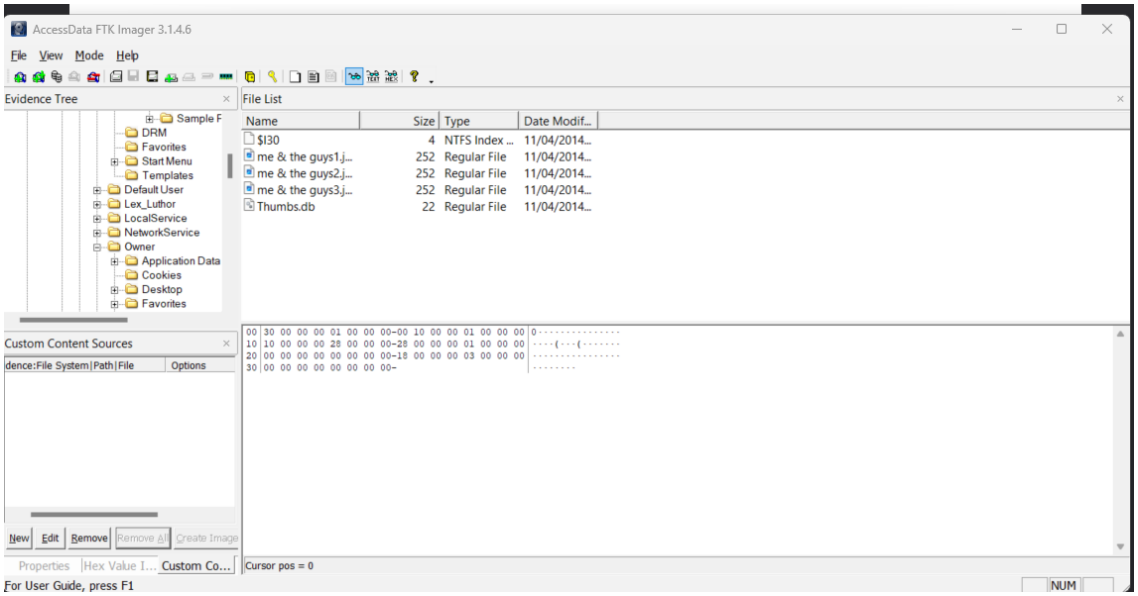
2. Select File > Add Evidence Item > Select Image File > Browse to Vader_Home_Computer.001
image and add it.



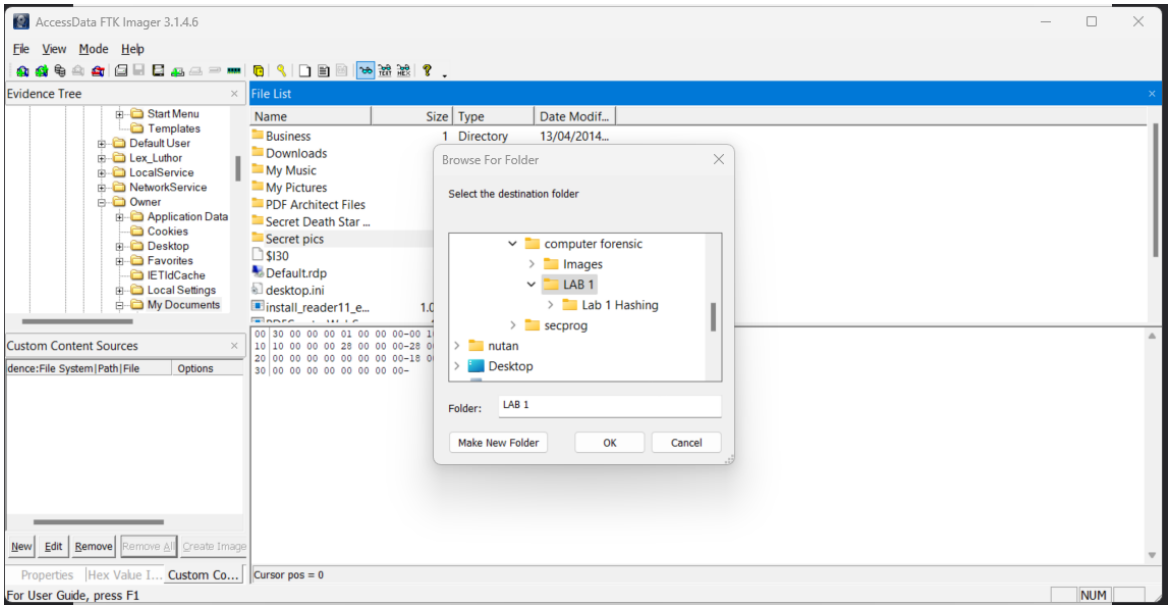


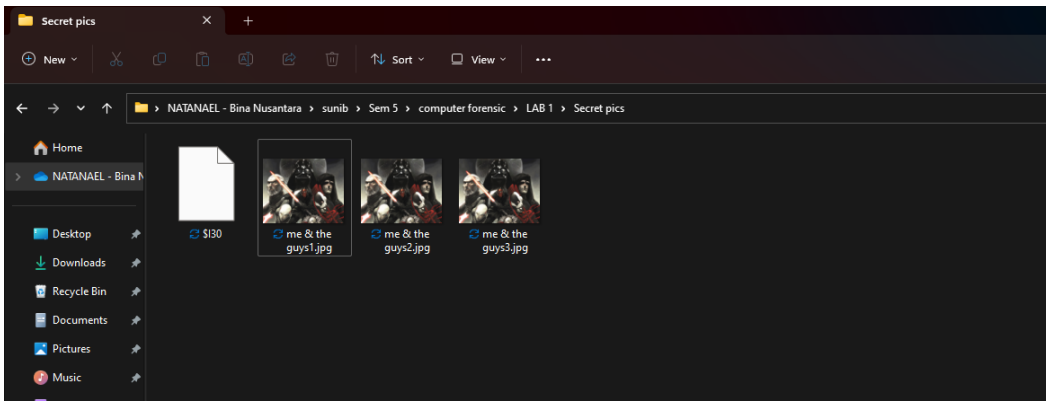


3. Navigate to the C:\Documents and Settings\Owner\My Documents\Secret pics folder.

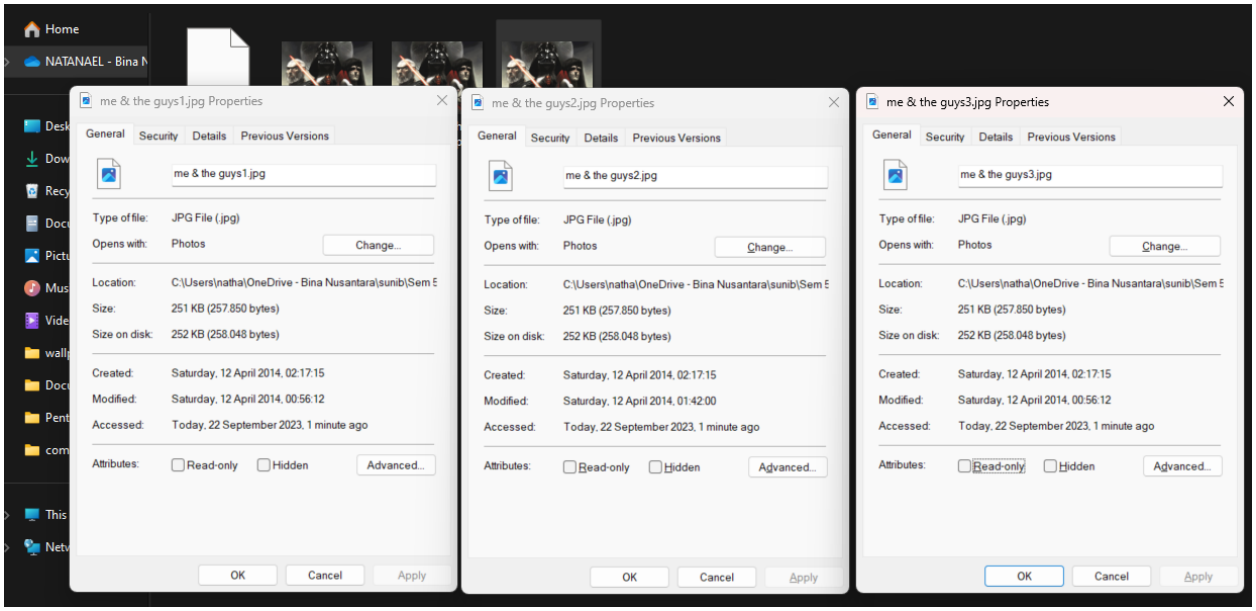


4. Export the “Secret Pics” folder to your local hard drive.





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)

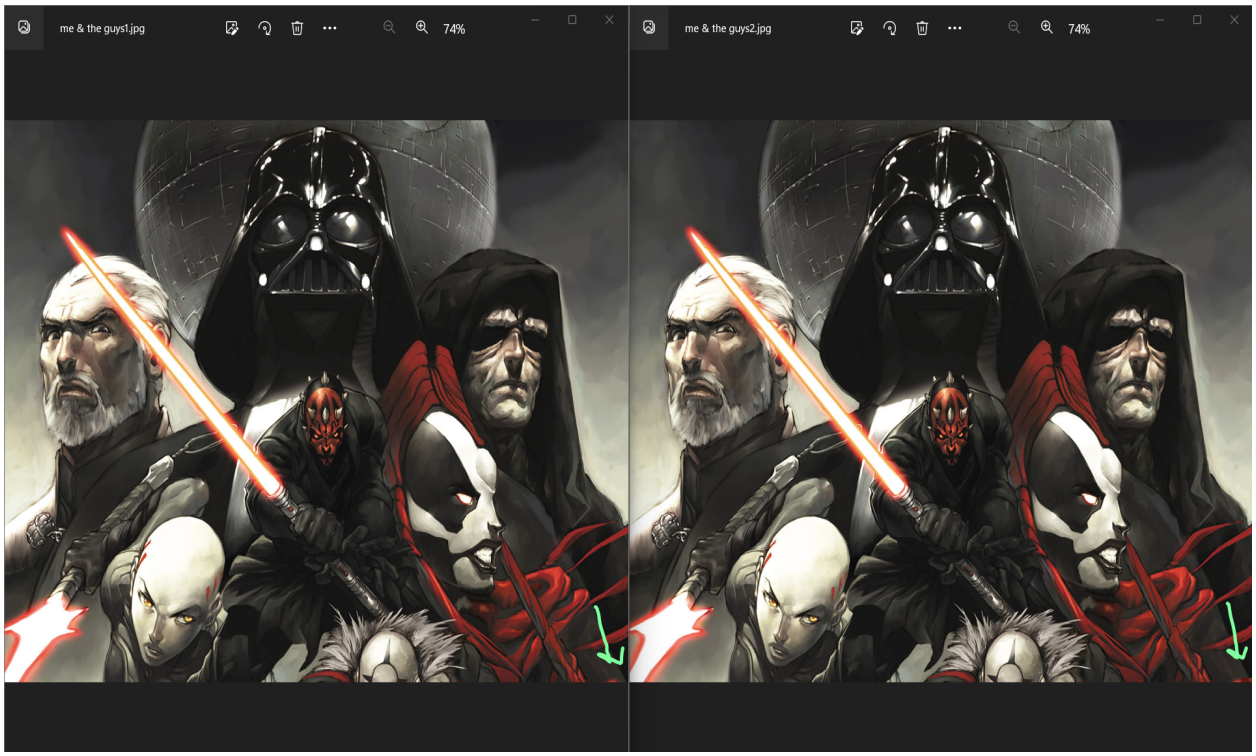


6. Open each image and describe the contents.
me & the guys1.jpg Description: gambar berupa 4 tokoh antagonist dari seri star wars yang cocok dengan nama dari image yaitu *vader's home computer* karena merupakan nama salah satu antagonistnya yang ada di gambar tetapi tidak ada yang aneh tentang gambar.

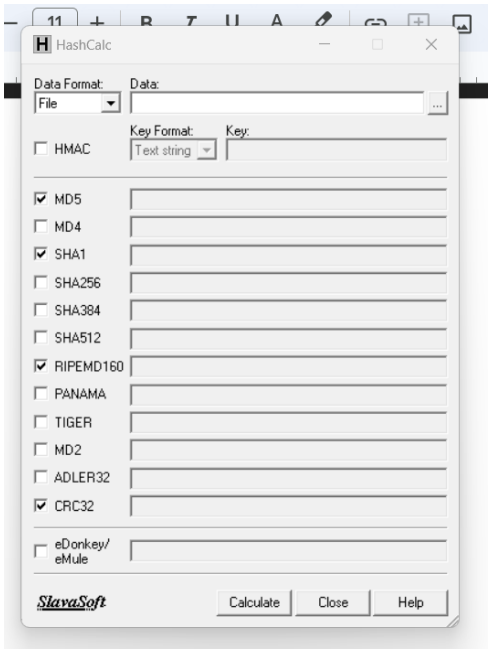
me & the guys2.jpg Description: gambar kedua adalah gambar yang sama dengan yang gambar 1 hanya saja terdapat seperti pergeseran dari gambar pertama.

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.

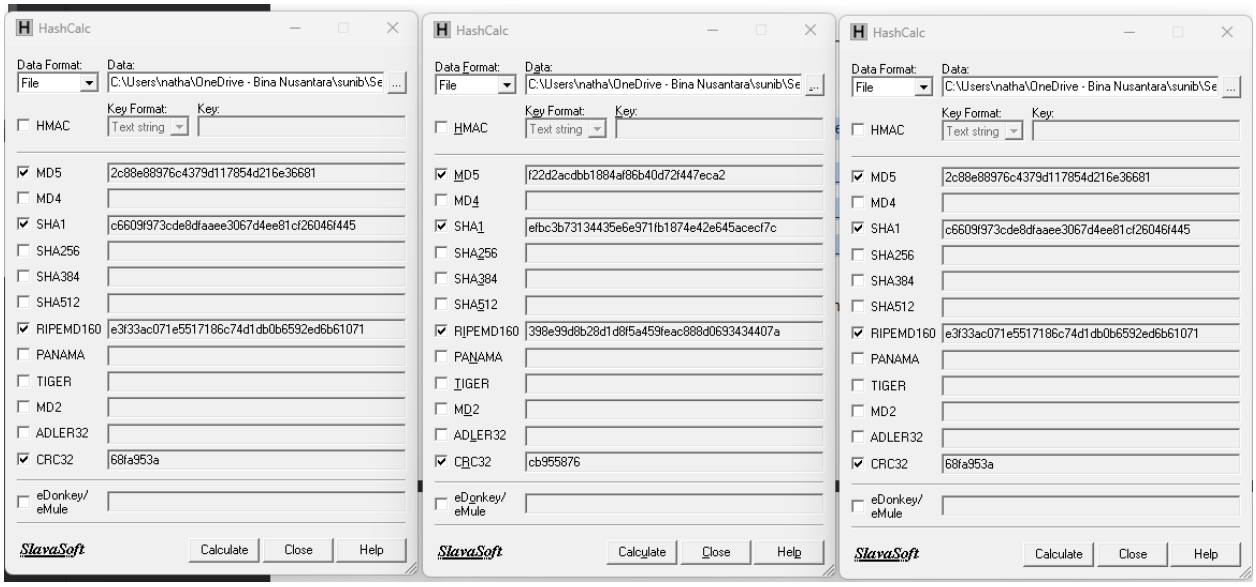
7. Are the pictures all identical?
Sepertinya tidak gambar 1 dan 3 terlihat mirip tetapi gambar 2 ada kejanggalan di pojok kanan bawah.



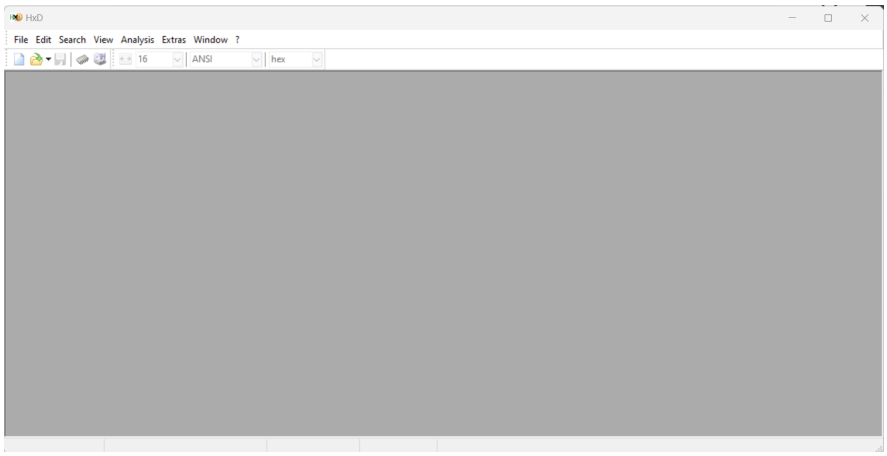
8. Install Hashcalc.exe.



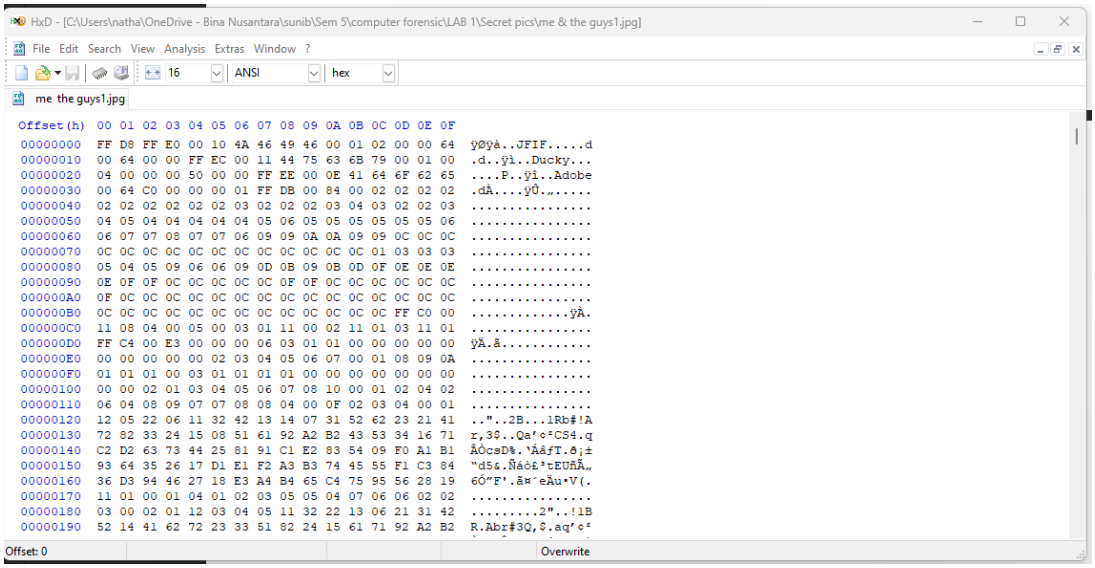
9. Use Hashcalc to calculate the hashes of all 3 files. Record the Md5 Hash value for each file.
me & the guys1.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681
me & the guys2.jpg Md5 Hash: f22d2acdbb1884af86b40d72f447eca2
me & the guys3.jpg Md5 Hash: 2c88e88976c4379d117854d216e36681



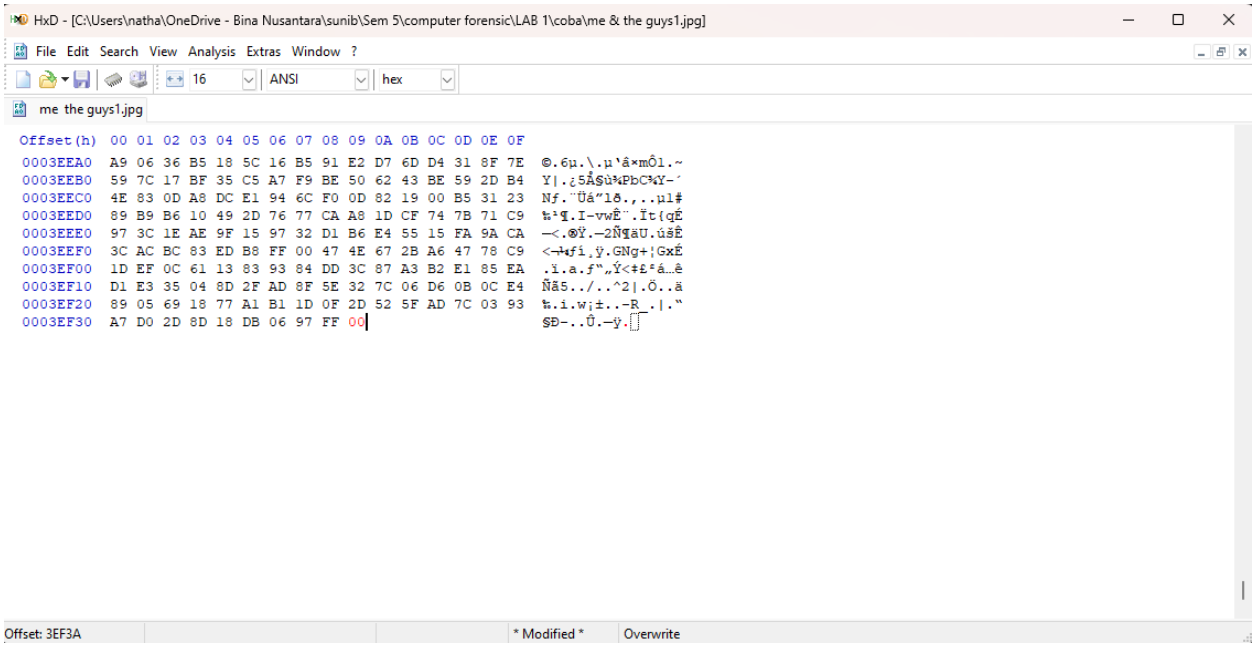
10. Install the HxD Hex Editor on your computer and open it.



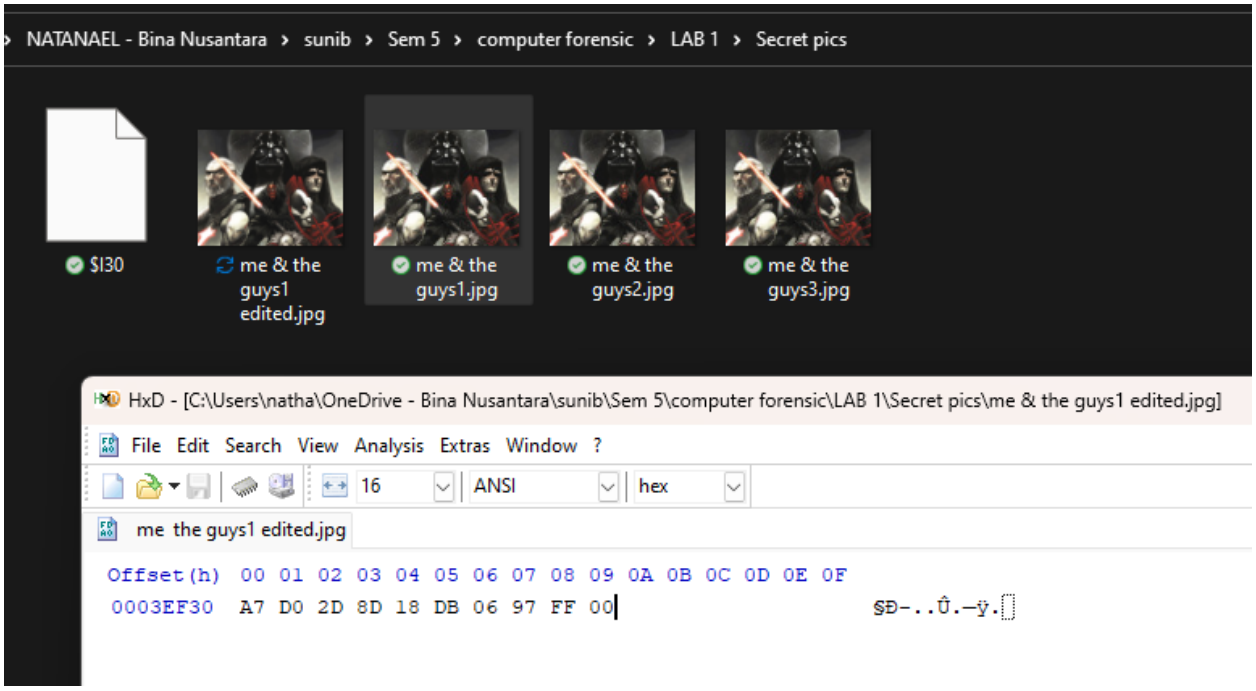
11. In HxD, select “open” under the file menu. Open one of 2 duplicate files. You know they are duplicate because they have an identical hash.



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.



14. Use Windows to record the file size and hash calc for the md5 hash of the new file.

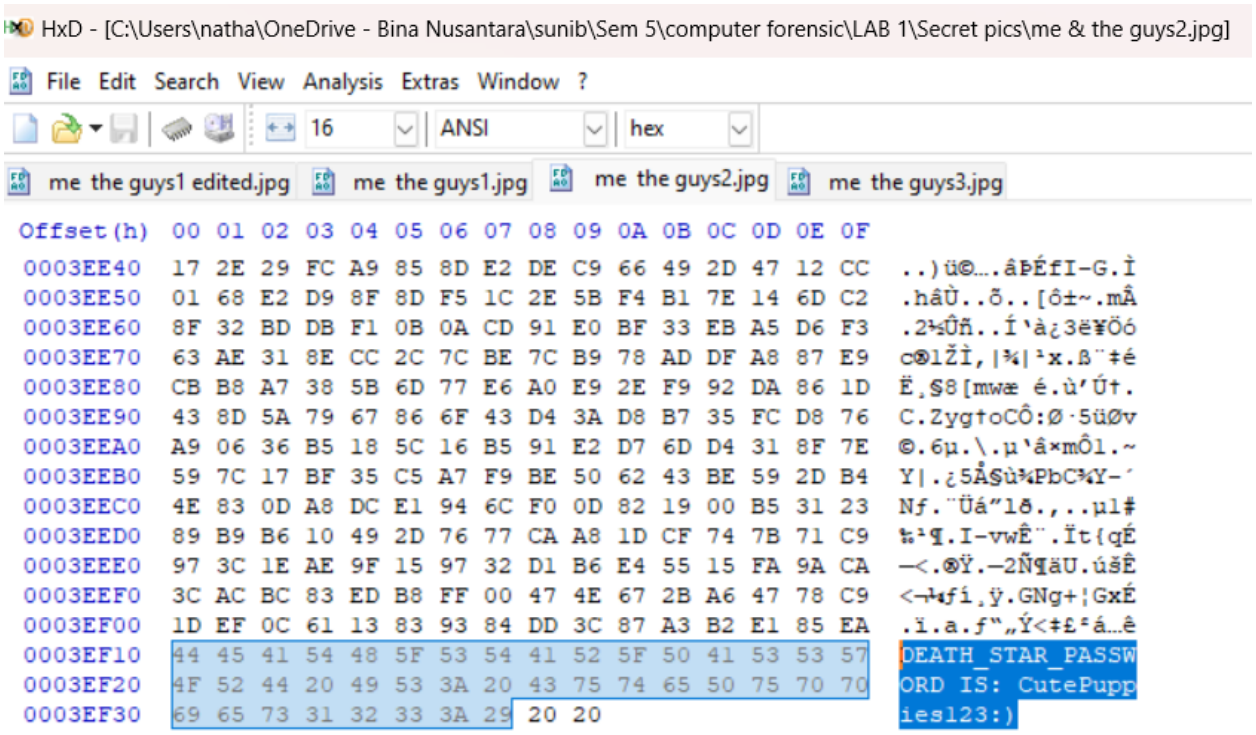
New File: me & the guys1 edited.jpg

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.



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.