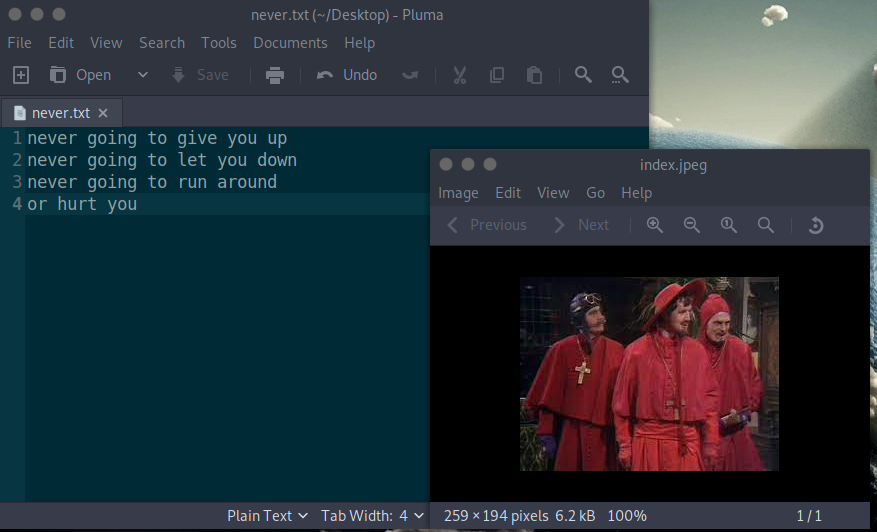
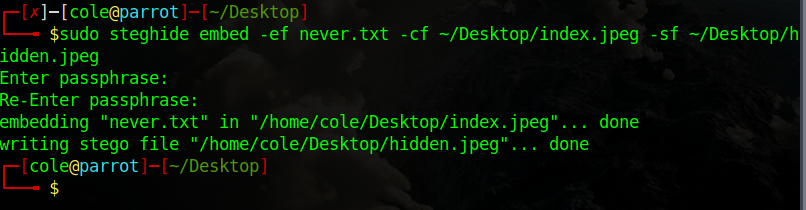
Part 1:

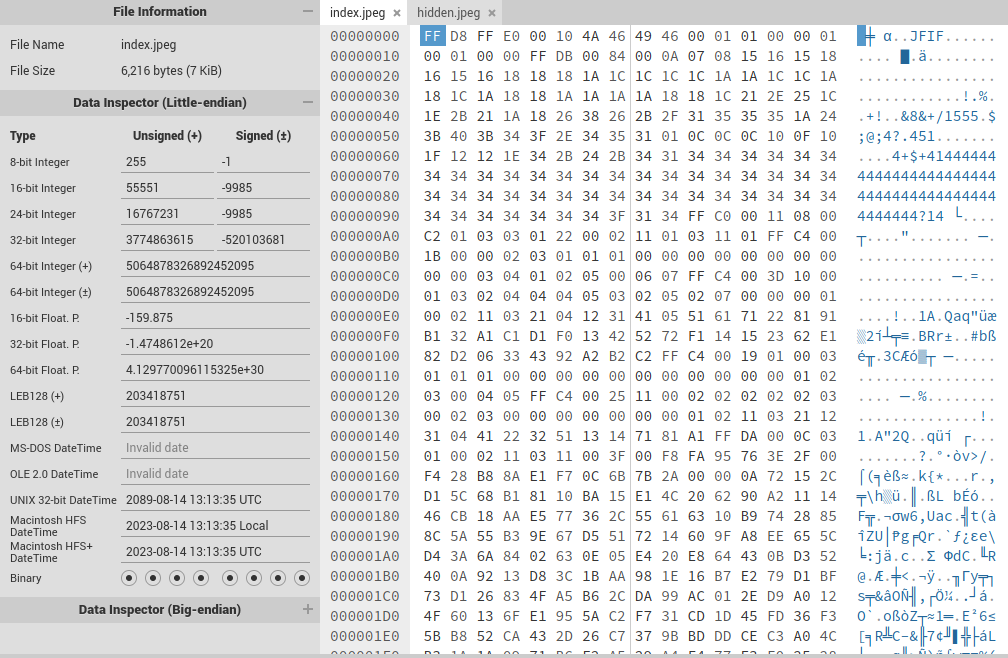
This is the image I selected and the text file im going to embed in it.

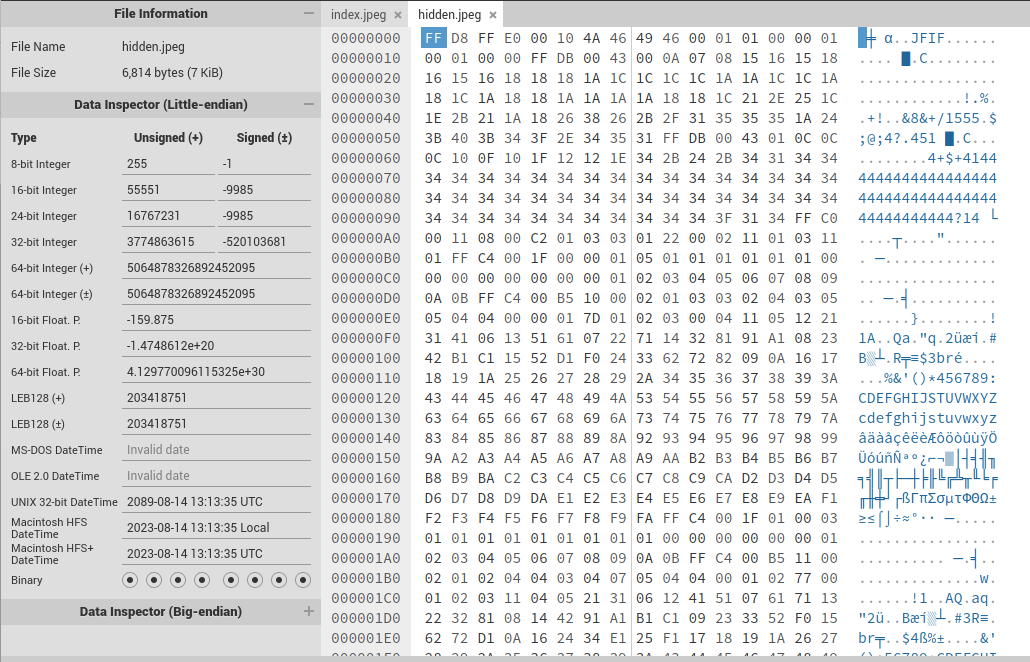


This is me using steghide to embed the file



Part 2:

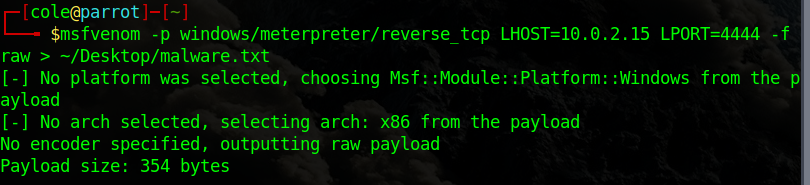




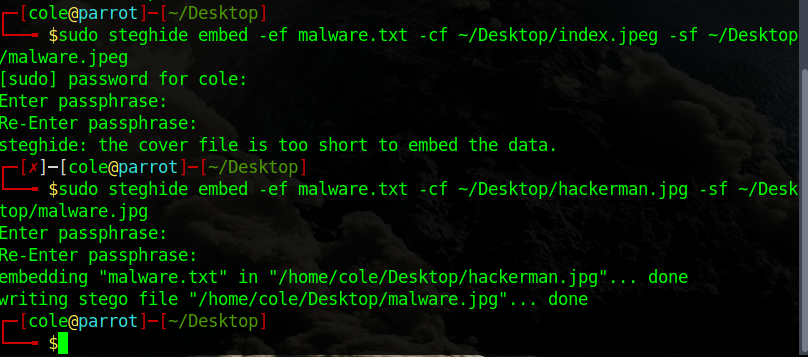
This is the comparison between the original image and the embedded image, as you can see the embedded image is larger and has differences in the hex dump.

Part 3:

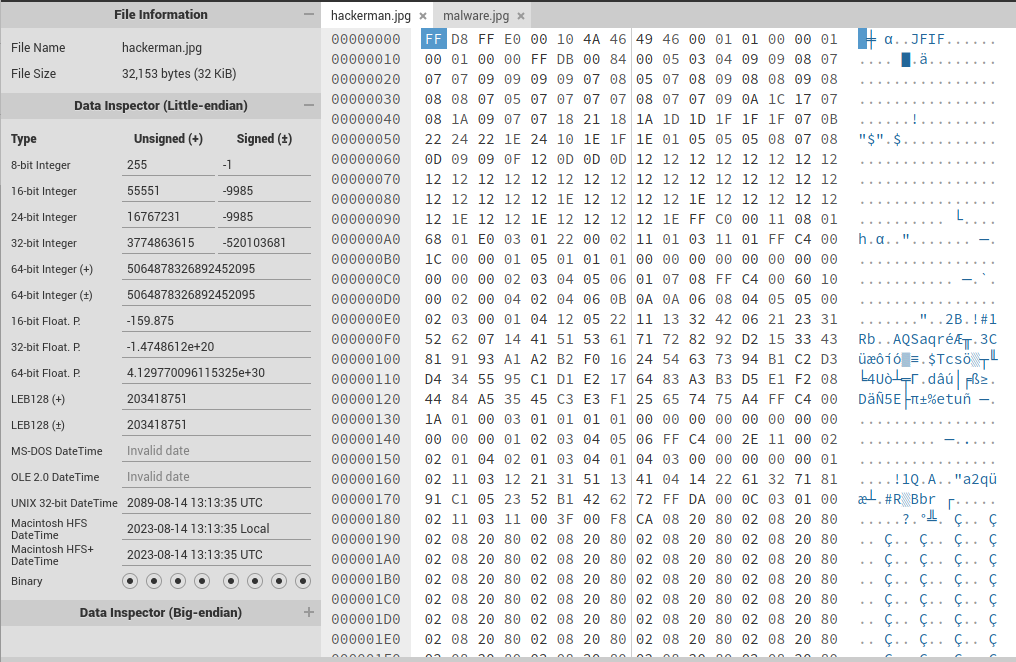
Here I created the payload file

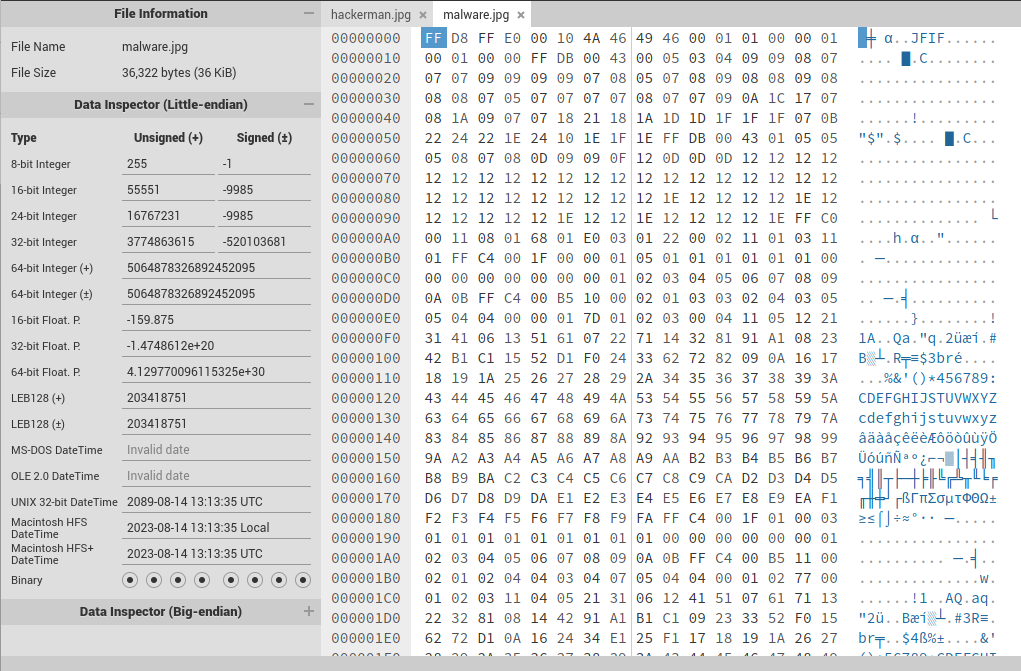


And here I embedded it in an image, I had to use a new one as the old one I used before was too small.



Part 4:

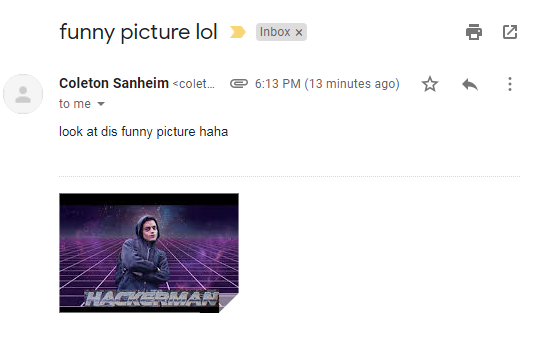




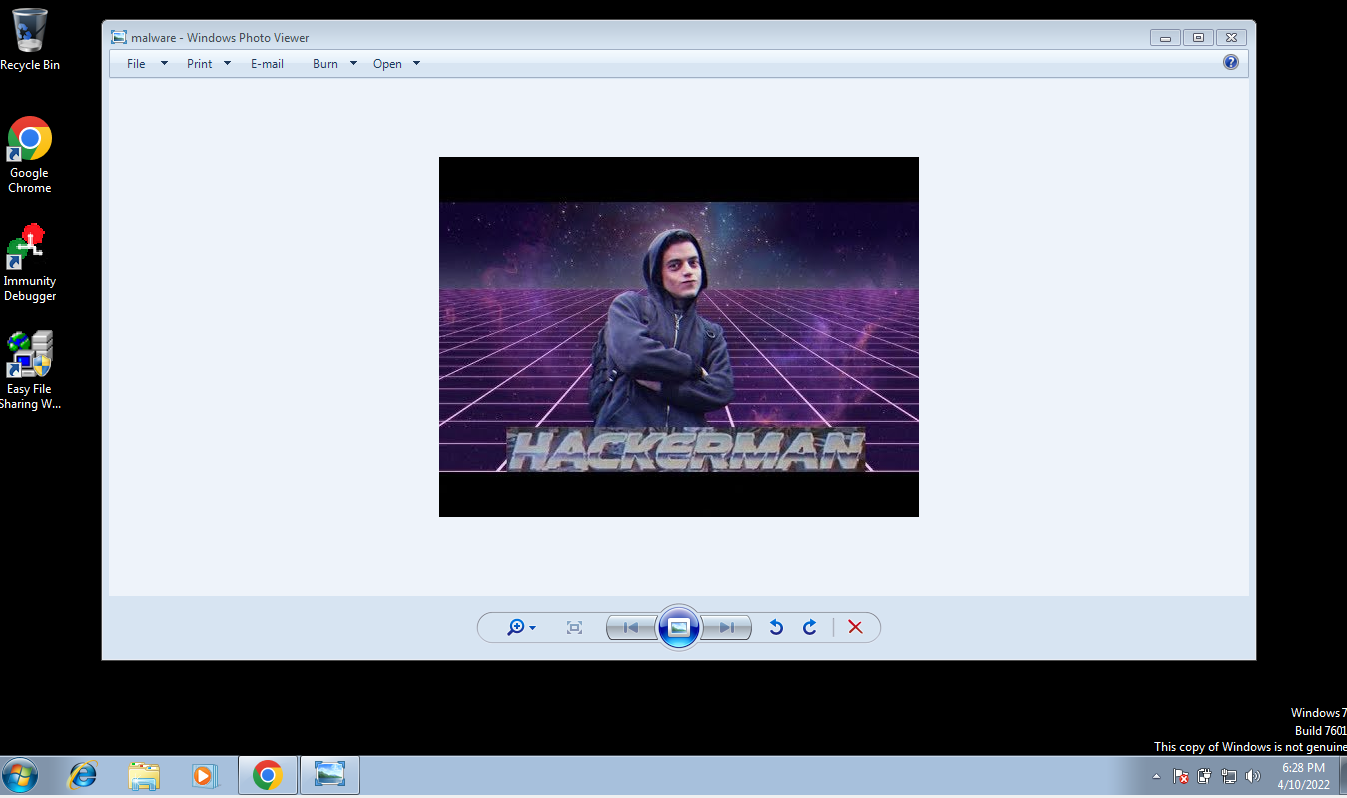
Again I compare the two images and the differences are the same as before.

Part 5:

Here is the phishing email I sent with the embedded infected image.



And here is it downloaded on the victim computer.



Now the implications of this are not very scary. IF someone sent an image that was infected and IF someone was dumb enough to download it, they would still have to somehow extract the embedded steganographic code and then somehow run it for it to compromise the machine. Overall as far as attacks go, this does not seem like an effective one.