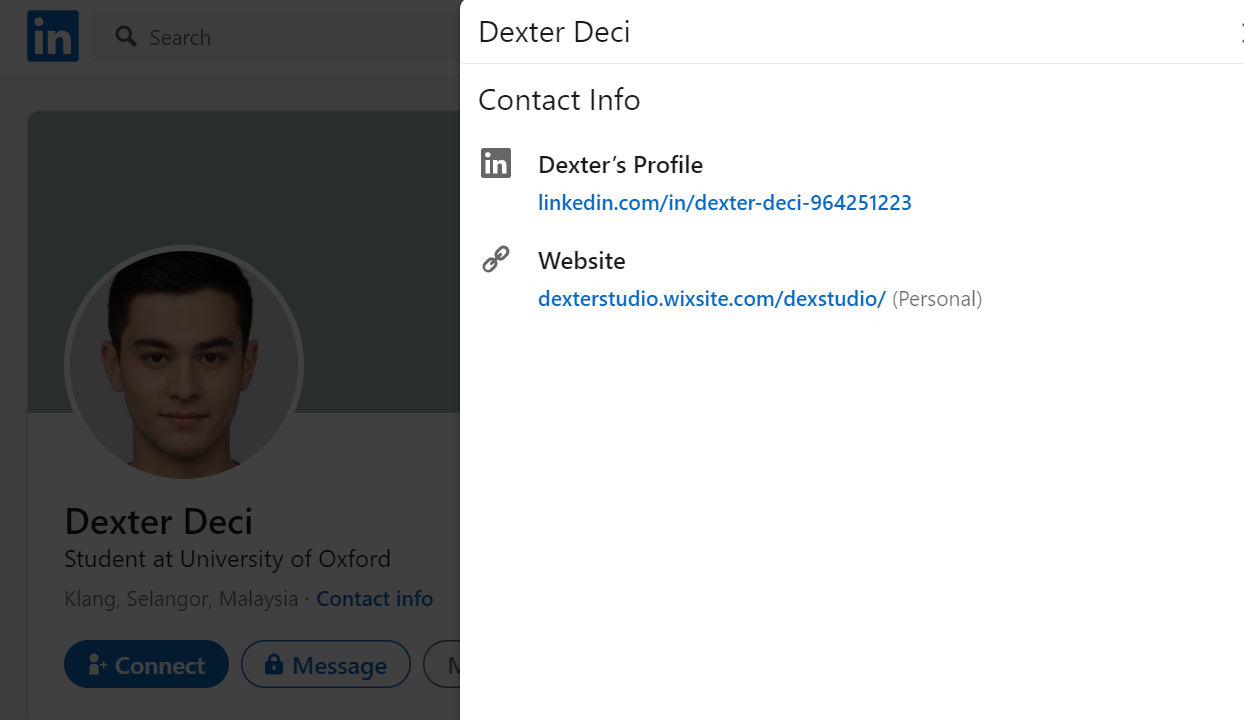
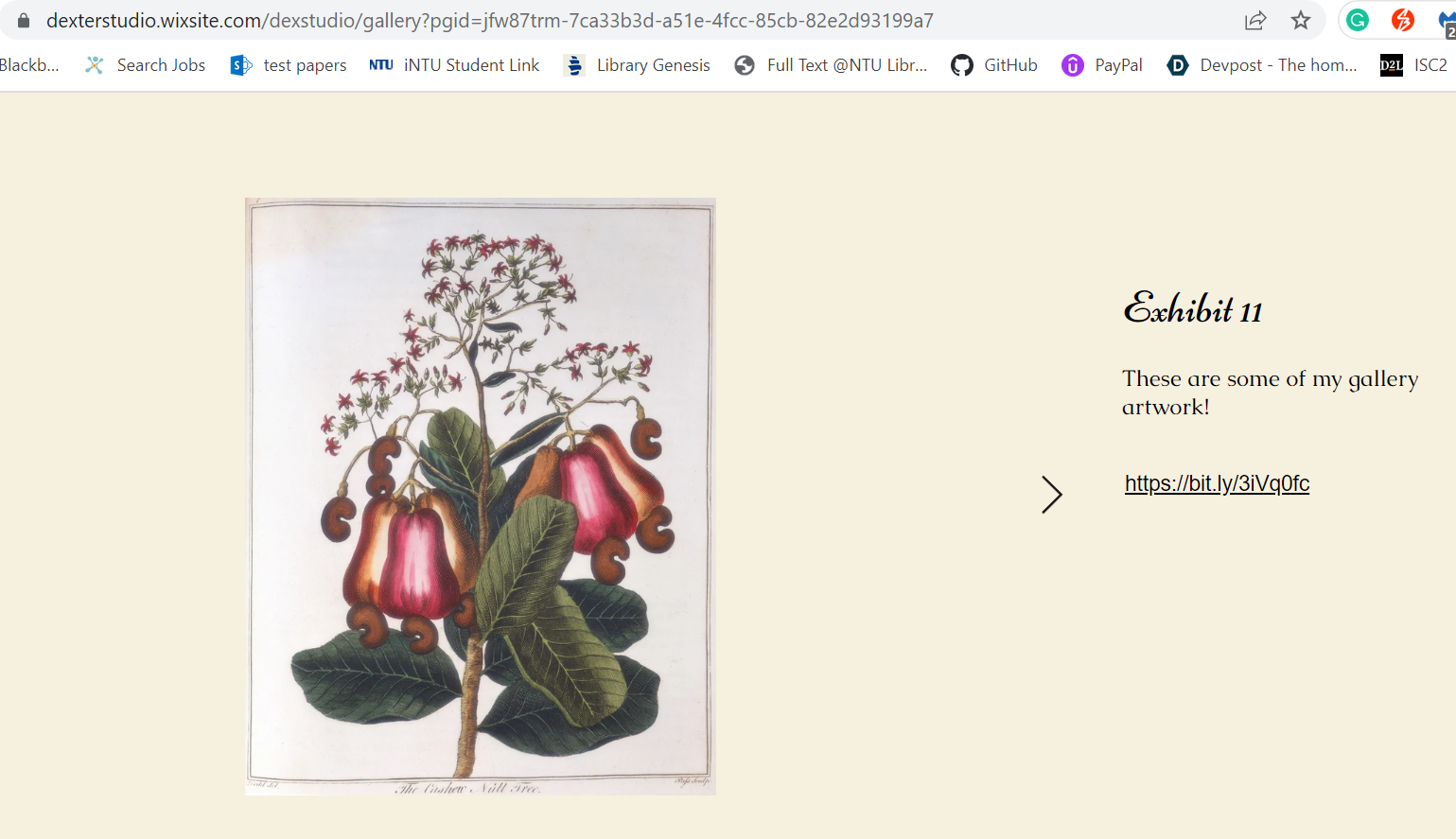
Search for ‘Dexter Deci’ on linkedin and click on his personal website.

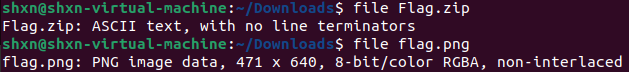


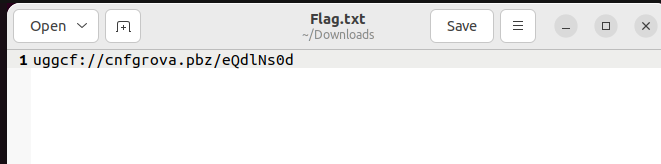
Explore his website and you will come across exhibit 11 whose description has a link (<https://bit.ly/3iVq0fc>) - > brings you to a google drive -> Downloads a zip folder



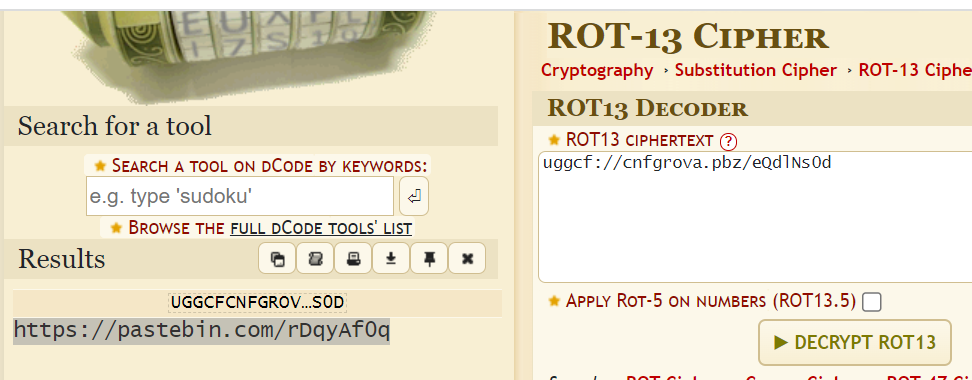
However, the zip folder cannot be extracted ; Not actually a zip folder

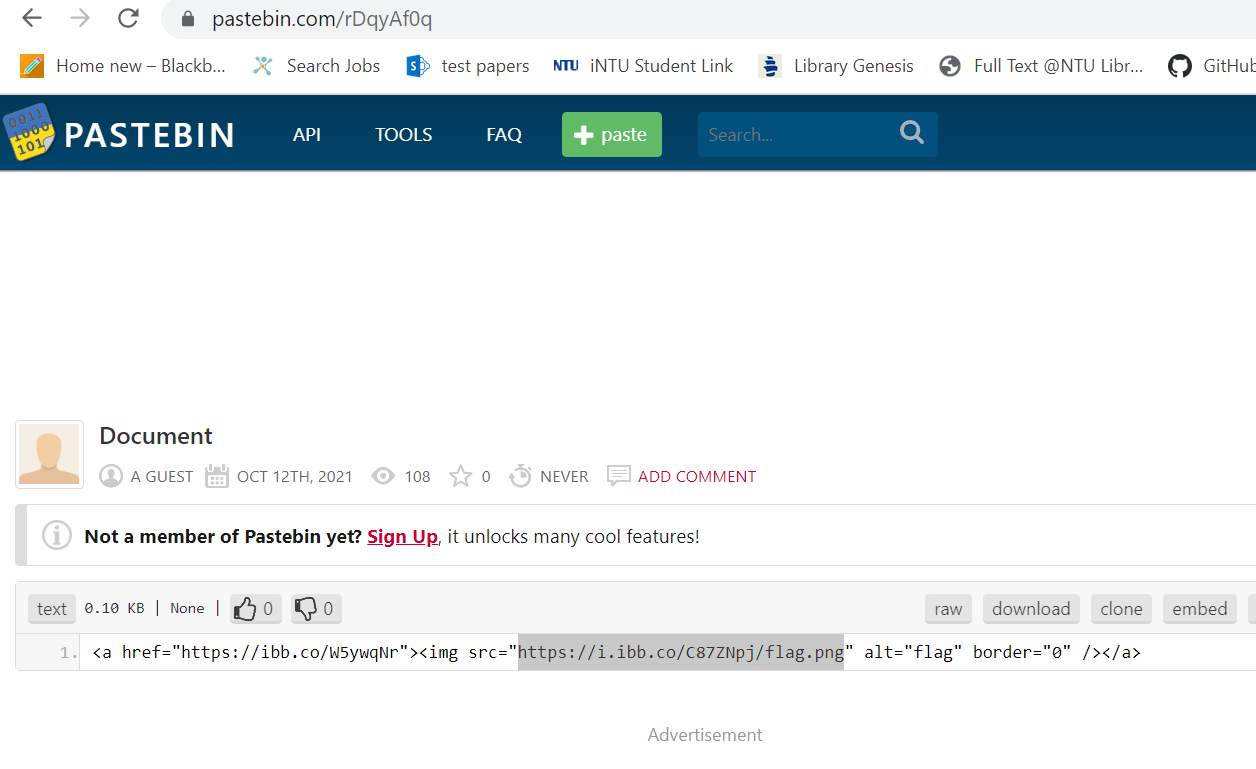
So check for its file type. It’s actually a text file -> rename the file to Flag.txt



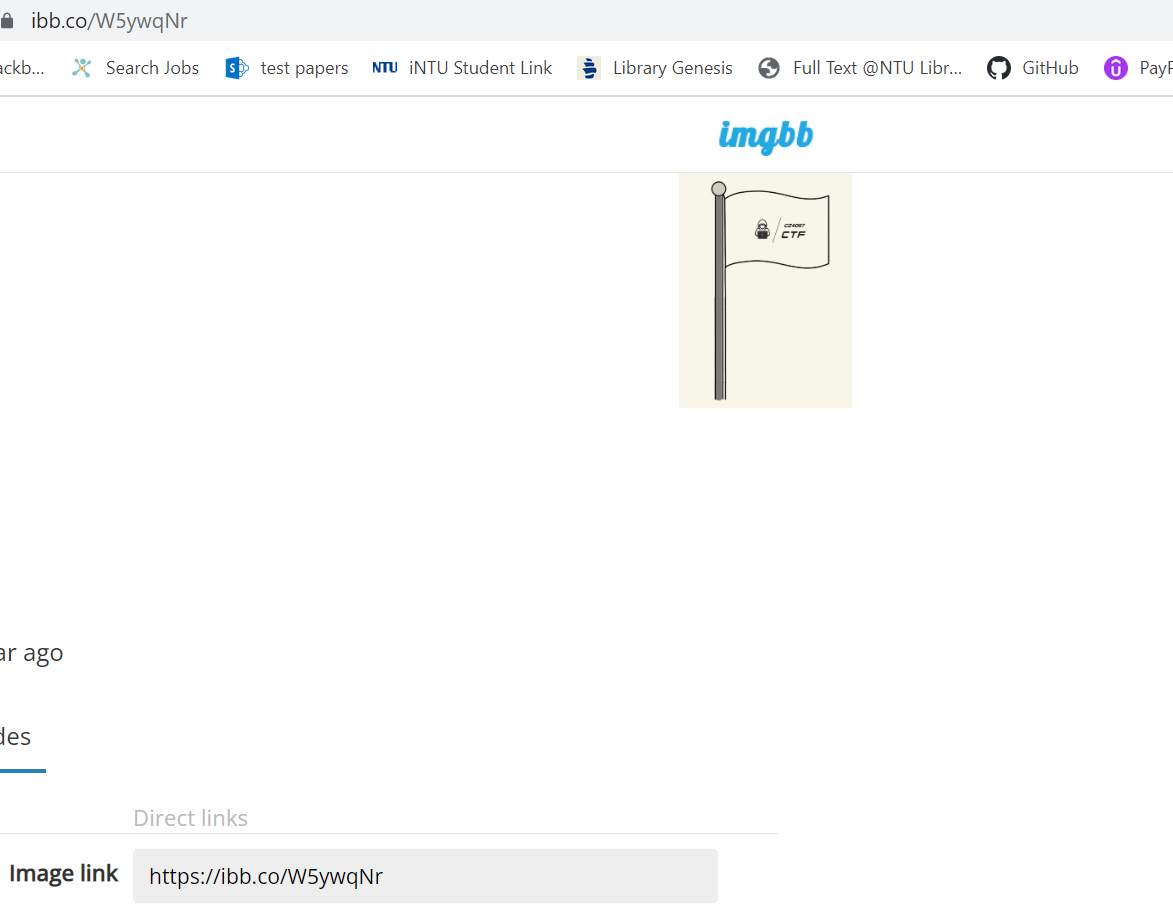
Open Flag.txt and we see a link:  


Decode this link using ROT-13 cipher -> Decoded string: https://pastebin.com/rDqyAf0q

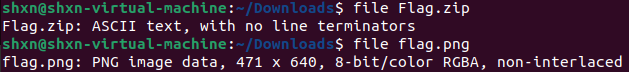


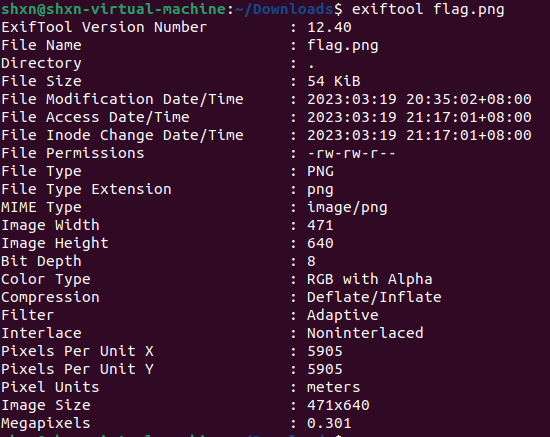
Go to the link and we see some html code posted by a guest user. Go to that link  


It brings us to a website that shows us an image of the flag.



Download the image and check its metadata. Seems fine, nothing suspicious





Tune the image’s and uncover the hidden bits (<https://incoherency.co.uk/image-steganography/#unhide>)



Flag: CZ4067{1\_aM-1nv1sibLe}