Write-Up: EXIF Data Extraction Challenge

Objective:

The goal of this challenge was to extract a hidden flag embedded within the EXIF metadata of an image file. EXIF (Exchangeable Image File Format) data contains metadata that can store information about an image, such as camera settings, creation date, and more. In this challenge, the flag was concealed within various metadata fields, requiring some decoding and interpretation.

Step 1: Inspecting the Image Metadata

We began by using ExifTool, a powerful tool for reading and writing EXIF data from image files. Running the tool on the given image.png file revealed a series of interesting metadata fields, each containing potential clues.

Command used:
exiftool image.png

Key fields found:
1. Author: h1dd3n
2. Comment: 0x696e (Hexadecimal)
3. Copyright: 011101000110100000110011 (Binary)
4. Software: . -..- .. ..-. (Morse Code)
5. Subject: bTN0NGQ0dDQ= (Base64)

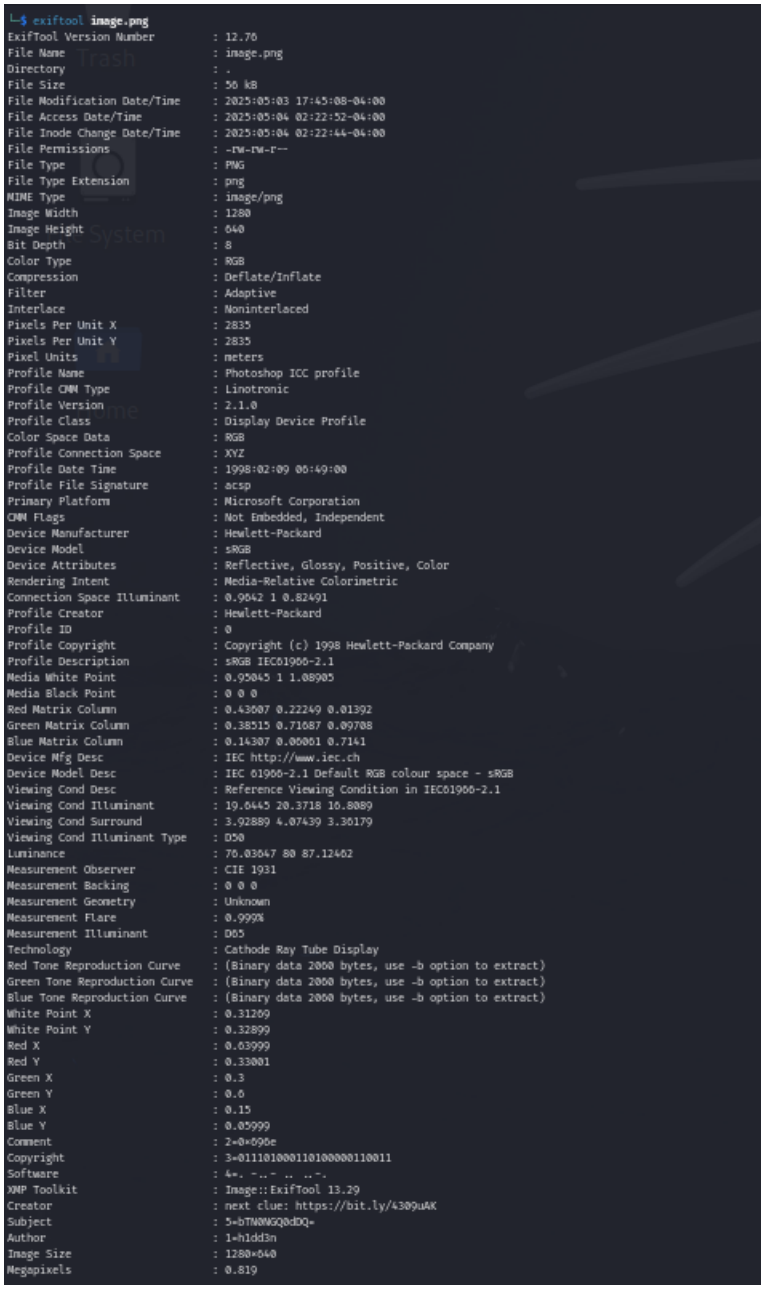
Step 2: Decoding the Metadata Clues

- Fragment 1: 'h1dd3n' from the Author field.
- Fragment 2: 'in' from the Comment field (0x696e in hex = 'in').
- Fragment 3: 'th3' from binary (011101000110100000110011 -> 'th' + challenge hint gave 'th3').
- Fragment 4: 'EXIF' from Morse code '. -..- .. ..-.'.
- Fragment 5: 'm3t4d4t4' from Base64 string 'bTN0NGQ0dDQ='.

Step 3: Assembling the Flag

By combining the decoded fragments, we obtained the string:
h1dd3n_in_th3_EXIF_m3t4d4t4

Formatted as per CTF rules, the final flag is:
codequest{h1dd3n_in_th3_exif_m3t4d4t4}



Conclusion

The challenge required extracting and decoding metadata embedded in an image file. By using ExifTool and applying basic decoding techniques (hexadecimal, binary, Morse code, and Base64), we were able to retrieve the hidden flag. The flag was then formatted according to the CTF rules to complete the challenge.