

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}

```
L$ exiftool image.png
ExifTool Version Number      : 12.70
File Name                    : image.png
Directory                   : .
File Size                    : 50 kB
File Modification Date/Time   : 2025:05:03 17:45:08+04:00
File Access Date/Time        : 2025:05:04 02:22:52+04:00
File Inode Change Date/Time   : 2025:05:04 02:22:44+04:00
File Permissions              : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 1280
Image Height                 : 640
Bit Depth                   : 8
Color Type                   : RGB
Compression                  : Deflate/Inflate
Filter                       : Adaptive
Interlace                    : Noninterlaced
Pixels Per Unit X            : 2835
Pixels Per Unit Y            : 2835
Pixel Units                  : meters
Profile Name                  : Photoshop ICC profile
Profile CMY Type              : Linotronic
Profile Version               : 2.1.0
Profile Class                 : Display Device Profile
Color Space Data              : RGB
Profile Connection Space      : XYZ
Profile Date Time             : 1998:02:09 00:49:00
Profile File Signature        : acsp
Primary Platform              : Microsoft Corporation
CMY Flags                     : Not Embedded, Independent
Device Manufacturer           : Hewlett-Packard
Device Model                  : sRGB
Device Attributes              : Reflective, Glossy, Positive, Color
Rendering Intent              : Media-Relative Colorimetric
Connection Space Illuminant   : 0.9542 1 0.82491
Profile Creator                : Hewlett-Packard
Profile ID                    : 0
Profile Copyright             : Copyright (c) 1998 Hewlett-Packard Company
Profile Description            : sRGB IEC61900-2.1
Media White Point              : 0.95045 1 1.08905
Media Black Point             : 0 0 0
Red Matrix Column              : 0.43607 0.22249 0.01392
Green Matrix Column            : 0.38515 0.71687 0.09708
Blue Matrix Column             : 0.14307 0.00001 0.7141
Device Mfg Desc                : IEC http://www.iec.ch
Device Model Desc              : IEC 61900-2.1 Default RGB colour space - sRGB
Viewing Cond Desc              : Reference Viewing Condition in IEC61900-2.1
Viewing Cond Illuminant       : 19.0445 20.3718 10.8089
Viewing Cond Surround          : 3.02889 4.07439 3.36179
Viewing Cond Illuminant Type   : D50
Luminance                     : 70.83647 80 87.12462
Measurement Observer           : CIE 1931
Measurement Backing            : 0 0 0
Measurement Geometry           : Unknown
Measurement Flare               : 0.999%
Measurement Illuminant         : D65
Technology                     : Cathode Ray Tube Display
Red Tone Reproduction Curve    : (Binary data 2000 bytes, use -b option to extract)
Green Tone Reproduction Curve  : (Binary data 2000 bytes, use -b option to extract)
Blue Tone Reproduction Curve   : (Binary data 2000 bytes, use -b option to extract)
White Point X                  : 0.31269
White Point Y                  : 0.32899
Red X                          : 0.63999
Red Y                          : 0.33001
Green X                        : 0.3
Green Y                        : 0.6
Blue X                         : 0.15
Blue Y                         : 0.05999
Comment                        : 2=0=090e
Copyright                     : 3=0111010001101000000110011
Software                       : 4= " " " " " " " " " "
XMP Toolkit                    : Image::ExifTool 13.29
Creator                        : next clue: https://bit.ly/4309uAK
Subject                        : 5=b7MNMQ08dQ=
Author                         : 1=h1dd3n
Image Size                    : 1280x640
Megapixels                     : 0.819
```

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.