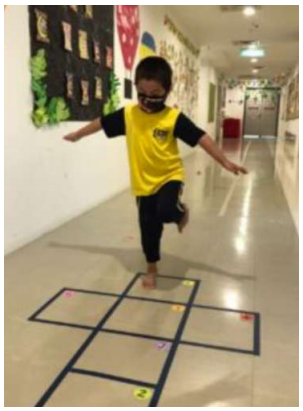
BAT--Bin has been playing all day

Sunday, March 16, 2025 1:20 PM



Extract Metadata:

- The image contains metadata, specifically a Comment field that holds encrypted text. To view the comment metadata, run the following command:

```
┌──(kali㉿kali)-[~/Desktop/CTF BAT/challenge files (Bin has been playing all day)]
└─$ exiftool teng-teng.png
ExifTool Version Number         : 12.76
File Name                       : teng-teng.png
Directory                       : .
File Size                       : 273 kB
File Modification Date/Time     : 2024:10:07 03:09:44-04:00
File Access Date/Time           : 2025:03:16 00:35:54-04:00
File Inode Change Date/Time     : 2025:03:16 00:35:30-04:00
File Permissions                : -rwxrw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 368
Image Height                    : 501
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
SRGB Rendering                  : Perceptual
Gamma                           : 2.2
Pixels Per Unit X               : 3779
Pixels Per Unit Y               : 3779
Pixel Units                     : meters
Comment                         : fe685a7aa83947125bd66e643d1b695ccee76f40f8534e30a7ee8fdeed5a928f380ab3a0ef7466c162c8ae4fdc2c79f6
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 368×501
Megapixels                      : 0.184
```

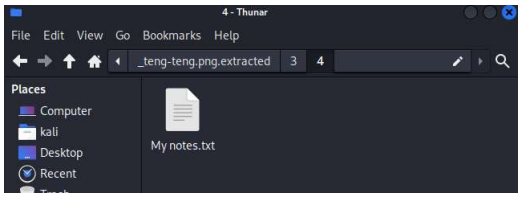
```
┌──(kali㉿kali)-[~/Desktop/CTF BAT/challenge files (Bin has been playing all day)]
└─$ exiftool teng-teng.png | grep Comment
Comment                         : fe685a7aa83947125bd66e643d1b695ccee76f40f8534e30a7ee8fdeed5a928f380ab3a0ef7466c162c8ae4fdc2c79f6
```

Extract Embedded Files:

The image also contains files embedded within it. To extract these files, use

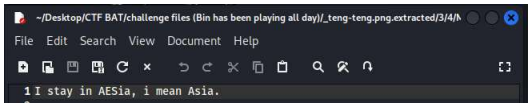
```
┌──(kali㉿kali)-[~/Desktop/CTF BAT/challenge files (Bin has been playing all day)]
└─$ binwalk -e teng-teng.png
/usr/lib/python3/dist-packages/binwalk/core/magic.py:431: SyntaxWarning: invalid escape sequence '\.'
  self.period = re.compile("\.")

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 368 x 501, 8-bit/color RGBA, non-interlaced
207           0×CF            Zlib compressed data, compressed
268466        0×418B2         Zip archive data, at least v2.0 to extract, name: 1/1/
268500        0×418D4         Zip archive data, at least v2.0 to extract, name: 1/2/
268534        0×418F6         Zip archive data, at least v2.0 to extract, name: 1/3/
268568        0×41918         Zip archive data, at least v2.0 to extract, name: 1/4/
268602        0×4193A         Zip archive data, at least v2.0 to extract, name: 1/5/
268636        0×4195C         Zip archive data, at least v2.0 to extract, name: 2/1/
268670        0×4197E         Zip archive data, at least v2.0 to extract, name: 2/2/
268704        0×419A0         Zip archive data, at least v2.0 to extract, name: 2/3/
268738        0×419C2         Zip archive data, at least v2.0 to extract, name: 2/4/
268772        0×419E4         Zip archive data, at least v2.0 to extract, name: 2/5/
268806        0×41A06         Zip archive data, at least v2.0 to extract, name: 3/1/
268840        0×41A28         Zip archive data, at least v2.0 to extract, name: 3/2/
268874        0×41A4A         Zip archive data, at least v2.0 to extract, name: 3/3/
268908        0×41A6C         Zip archive data, at least v2.0 to extract, name: 3/4/
268942        0×41A8E         Zip archive data, at least v2.0 to extract, compressed size: 169, uncompressed size: 1455, name: 3/4/My notes.txt
269157        0×41B65         Zip archive data, at least v2.0 to extract, name: 3/5/
269191        0×41B87         Zip archive data, at least v2.0 to extract, name: 4/1/
269225        0×41BA9         Zip archive data, at least v2.0 to extract, name: 4/2/
269259        0×41BCB         Zip archive data, at least v2.0 to extract, name: 4/3/
269293        0×41BED         Zip archive data, at least v2.0 to extract, name: 4/4/
269327        0×41C0F         Zip archive data, at least v2.0 to extract, name: 4/5/
269361        0×41C31         Zip archive data, at least v2.0 to extract, name: 5/1/
269395        0×41C53         Zip archive data, at least v2.0 to extract, name: 5/2/
269429        0×41C75         Zip archive data, at least v2.0 to extract, name: 5/3/
269463        0×41C97         Zip archive data, at least v2.0 to extract, name: 5/4/
```

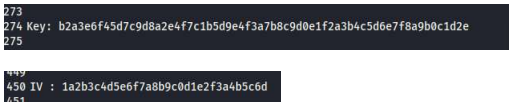
After Tree commend: there is a txt file in the fourth document in the third folder, and there are two more zip files, 41882.zip and 42211.zip, and then a CF and CF.zlib.



Find the Key and IV:

Inside the extracted directory, you'll find a strange file named "my notes.txt". Opening this file reveals a hint: "AESia," which points to the use of the ***AES encryption*** algorithm. ***AES requires both a key and an initialization vector (IV) to decrypt the text found in the metadata***.





Decrypt the Text:

Once you've gathered the key and IV, use the CyberChef tool to decrypt the encrypted text from the image's