Iera Milpan

1. Challenge Overview:

The challenge presents an MP3 file with potential hidden data embedded within it. The task is to identify and extract this hidden information. First thing I proceed to play the mp3 files using cyberchef and found nothing unusual in it.

- **File Type**: MP3 audio file
- **Challenge Type**: Forensics (likely steganography)

2. Check File Properties:

Use file analysis tools to inspect the MP3 file's metadata and structure.

- **Command (Linux): file <filename>.mp3**
    - This command reveals the general type of file and any anomalies. It could reveal if the file has any suspicious attributes (e.g., strange file size or additional extensions).
- **Command (Linux): exiftool <filename>.mp3**
    - ExifTool can show metadata embedded in the MP3 file (ID3 tags, artist, title, album, etc.). Hidden data could be in the comments or other fields.

Output from **file**:

```
jen@LAPTOP-LU9615OC:~$ file Retak_Hatiku_-_Iera_Milpan.mp3
Retak_Hatiku_-_Iera_Milpan.mp3: PNG image data, 1219 x 48, 8-
bit/color RGBA, non-interlaced
jen@LAPTOP-LU9615OC:~$
```

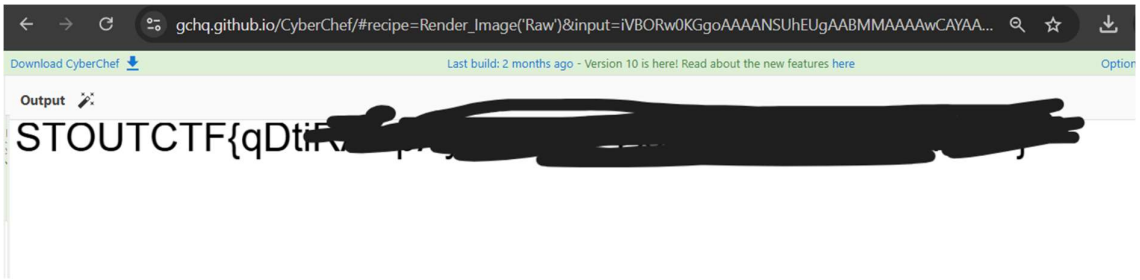
Output from **exiftool**:

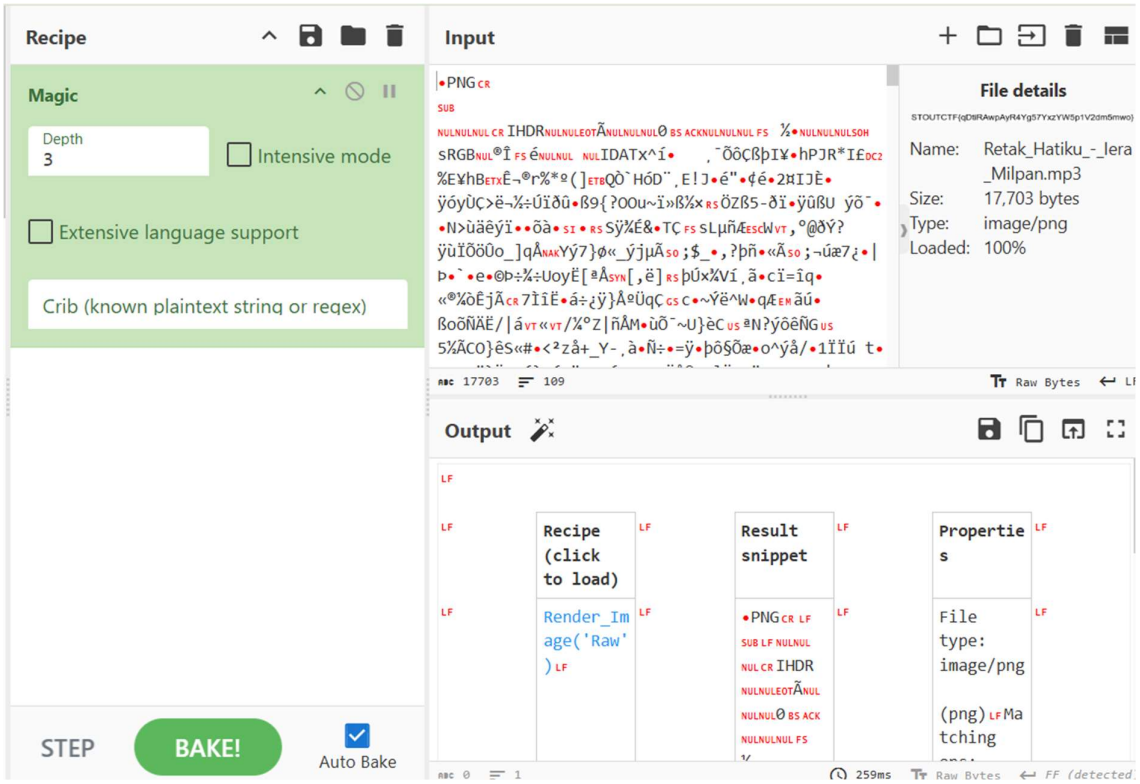
```
jen@LAPTOP-LU9615OC:~$ exiftool Retak_Hatiku_-_Iera_Milpan.mp
3
ExifTool Version Number         : 12.40
File Name                       : Retak_Hatiku_-_Iera_Milpan.
mp3
Directory                       : .
File Size                       : 17 KiB
File Modification Date/Time     : 2024:12:27 12:51:28+08:00
File Access Date/Time           : 2024:12:27 12:54:49+08:00
File Inode Change Date/Time     : 2024:12:27 12:54:24+08:00
File Permissions                : -rw-r--r--
File Type                       : MP3
File Type Extension             : mp3
MIME Type                       : audio/mpeg
MPEG Audio Version              : 2
Audio Layer                     : 3
Audio Bitrate                   : 56 kbps
Sample Rate                     : 16000
Channel Mode                    : Single Channel
MS Stereo                       : Off
Intensity Stereo                : On
Copyright Flag                  : True
Original Media                  : False
Emphasis                        : 50/15 ms
Duration                        : 2.53 s (approx)
```

3. Search for Hidden Data

MP3 Steganography and CyberChef Analysis

1. **Extract the Image from the MP3**:
   Using the **CyberChef "Magic"** operation and I got interesting result.
   - **Extract the embedded image**:
     1. Drag and drop the MP3 file into **CyberChef**.
     2. Apply the **"Magic"** operation (to identify the image).
     3. Once identified, extract the image content and save it as a separate file.


gchq.github.io/CyberChef/#recipe=Render_Image('Raw')&input=iVBORw0KGgoAAAANSUhEUgAABMMAAAAwCAYAA...
Download CyberChef
Last build: 2 months ago - Version 10 is here! Read about the new features here
Output
STOUTCTF{qDtiR


Recipe
Magic
Depth
3
Intensive mode
Extensive language support
Crib (known plaintext string or regex)
STEP
BAKE!
Auto Bake
Input
File details
Name: Retak_Hatiku_-_lera_Milpan.mp3
Size: 17,703 bytes
Type: image/png
Loaded: 100%
Output
Recipe (click to load)
Result snippet
Properties
Render_Image('Raw')
File type: image/png
(png) Matching ops: Parse QR Code, Raw Inflate, Render Image Useful op detected Entropy: 7.96


Output
Recipe (click to load)
Result snippet
Properties
Render_Image('Raw')
File type: image/png
(png) Matching ops: Parse QR Code, Raw Inflate, Render Image Useful op detected Entropy: 7.96
File type: image/png
(png) Matching ops: Parse QR Code, Raw Inflate, Render Image Entropy: 7.96

Then I proceed to click at Render_Image('Raw') and its reveal our flag!

Conclusion The hidden data was embedded in a **PNG** image inside the **MP3** file using steganography. By extracting the image and analyzing it with CyberChef and steganography tools, we successfully uncovered the flag.