CYS Report Cognizance Recruitment Task

Task 1: “This garden contains more than it seems”

Process

1. **Initial Analysis**:
    - The image appeared to be a normal garden scene with no apparent signs of alteration or hidden data.
2. **Using strings Command**:
    - The `strings` command, which extracts readable text from binary files, was employed.
    - Running this command on the image file revealed a hidden text string, which included the flag.

Flag Obtained

- **Flag**: `picoCTF{more_than_m33ts_the_3y3657BaB2C}`

Task 2: "Files can always be changed in a secret way"

Process

1. **Metadata Inspection**:
    - Using **ExifTool**, I examined the image’s metadata to find any hidden information.
    - I found a suspicious license string encoded in Base64 within the metadata.
2. **Base64 Decoding**:
    - The Base64 string was decoded, revealing the hidden flag within the metadata.

Flag Obtained

- **Flag**: `picoCTF{the_m3tadata_1s_modified}`

Task 3: “There will always be more than what it seems to contain”

Process

1. **Advanced Steganography Analysis**:
    - I used steganography tools such as **Binwalk** to analyze the image for hidden files or data.
    - **Binwalk** identified an embedded image within the original image file.
2. **Extracting the Hidden Image**:
    - I extracted the embedded image file, which contained the hidden flag.

Flag Obtained

- **Flag**: `picoCIF(Hiddinng_An_imag3_within_@n_image_96539bea)`

Summary of Flags

1. **Task 1**: `picoCTF{more_than_m33ts_the_3y3657BaB2C}`
2. **Task 2**: `picoCTF{the_m3tadata_1s_modified}`
3. **Task 3**: `picoCIF(Hiddinng_An_imag3_within_@n_image_96539bea)`