

Steganography

Pranav Mohanraj

Steganography Image Download Link -

https://drive.google.com/file/d/1nsZ97v4deyqJe4L367DJxLb0QL3MQrj5/view?usp=drive_link

Table of Contents

Introduction.....	3
1. Metadata Analysis of the Target Image Using ExifTool.....	4

Introduction

Steganography is the technique of concealing sensitive information within ordinary digital media such as images, audio, video, or text in a manner that prevents detection of the hidden data.

Unlike cryptography, which focuses on protecting the content of a message, steganography aims to hide the very existence of communication. This characteristic makes steganography a significant concept in cybersecurity, particularly in the areas of secure communication, digital forensics, and information security analysis.

In this documentation, a practical steganalysis exercise is conducted using a Kali Linux system with the IP address **192.168.28.130** as the analysis environment. The investigation focuses on the image file **Find_me_1577975566801.jpg**, which is examined for the presence of concealed or embedded information using standard steganalysis techniques and tools. This exercise demonstrates a structured approach to detecting and extracting hidden data from digital images, while highlighting the relevance of steganography and steganalysis in both offensive and defensive cybersecurity contexts.

1. Metadata Analysis of the Target Image Using ExifTool

```
(kali㉿kali)-[~/Steganography]
$ exiftool Find_me_1577975566801.jpg
ExifTool Version Number      : 13.36
File Name                   : Find_me_1577975566801.jpg
Directory                   :
File Size                    : 35 kB
File Modification Date/Time : 2025:12:09 04:02:35-05:00
File Access Date/Time       : 2025:12:09 04:04:02-05:00
File Inode Change Date/Time: 2025:12:09 04:04:02-05:00
File Permissions            : -rw-
File Type                   : JPEG
File Type Extension         : jpg
MIME Type                   : image/jpeg
JFIF Version                : 1.01
X Resolution                 : 96
Y Resolution                 : 96
Exif Byte Order              : Big-endian (Motorola, MM)
Resolution Unit              : inches
Y Cb Cr Positioning        : Centered
Exif Version                 : 0231
Components Configuration    : Y, Cb, Cr, -
Flashpix Version             : 0100
Owner Name                   : THM{3x1f_0r_3x1f} ←
Comment                      : CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 60.
Image Width                  : 800
Image Height                  : 480
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                    : 800x480
Megapixels                     : 0.384
```

The screenshot shows the use of the exiftool utility to analyze the metadata of the image **Find_me_1577975566801.jpg**. The output confirms that the file is a valid JPEG image with standard encoding properties. Notably, the metadata contains an **Owner Name** field with the value **ThM{3x1f_0r_3x1f}**, which appears to be intentionally embedded and formatted in a CTF-style flag pattern. In addition, the **Comment** field identifies the image creation software and compression quality, indicating that the image was processed using JPEG encoding tools. The presence of a flag-like value within the metadata represents **direct evidence of metadata-based steganography**, demonstrating that hidden information has been stored within the image's metadata rather than its pixel or file structure. This finding confirms successful concealment of data at the metadata level and justifies further documentation without requiring deeper structural or pixel-based analysis.