Steganography

Pranav Mohanraj

Steganography Image Download Link -

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

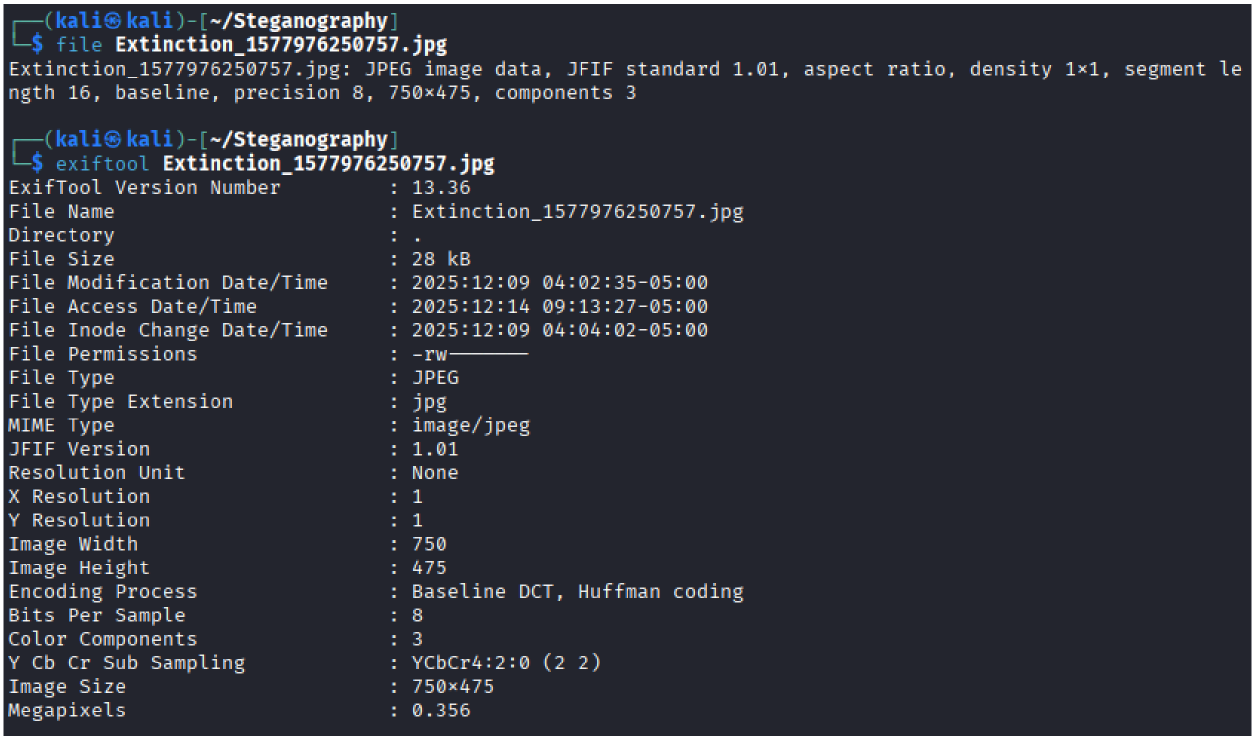
Table of Contents

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 **Extinction_1577976250757.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. Initial File and Metadata Analysis of the Target Image using EXIFTOOL

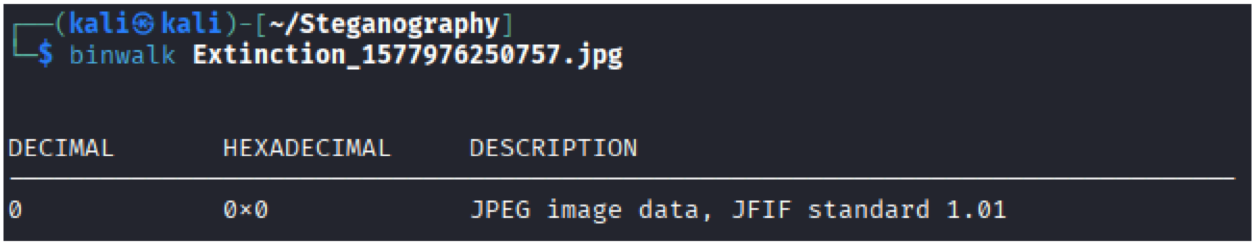


```
┌──(kali㉿kali)-[~/Steganography]
└─$ file Extinction_1577976250757.jpg
Extinction_1577976250757.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1×1, segment le
ngth 16, baseline, precision 8, 750×475, components 3

┌──(kali㉿kali)-[~/Steganography]
└─$ exiftool Extinction_1577976250757.jpg
ExifTool Version Number         : 13.36
File Name                       : Extinction_1577976250757.jpg
Directory                       : .
File Size                       : 28 kB
File Modification Date/Time     : 2025:12:09 04:02:35-05:00
File Access Date/Time           : 2025:12:14 09:13:27-05:00
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
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 750
Image Height                    : 475
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 750×475
Megapixels                      : 0.356
```

The screenshot shows the initial identification and metadata analysis of the image **Extinction_1577976250757.jpg** using the file and exiftool utilities. The file command confirms that the image is a valid JPEG file conforming to the JFIF standard, with baseline DCT encoding and standard image components. This establishes that the file structure is intact and suitable for further steganalysis. The subsequent exiftool output provides detailed image properties such as dimensions, encoding process, color sampling, and file size. No IPTC metadata, comments, or anomalous fields are observed at this stage, indicating that the image does not rely on metadata-based steganography. Based on these findings, further analysis is required to determine whether hidden data exists within the image structure or pixel data.

2. File Structure Analysis Using Binwalk

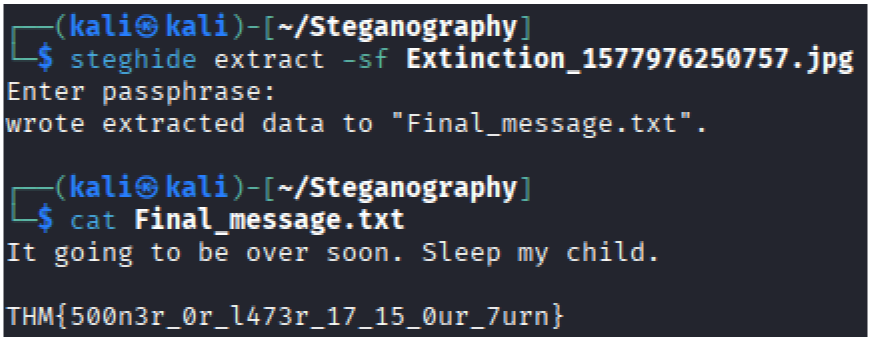


```
┌──(kali㉿kali)-[~/Steganography]
└─$ binwalk Extinction_1577976250757.jpg


DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

The screenshot shows the use of the binwalk tool to analyze the internal structure of the image **Extinction_1577976250757.jpg**. The output confirms that the file contains only standard JPEG image data conforming to the JFIF 1.01 specification. No embedded archives, compressed payloads, or appended data structures were detected during the analysis. This result indicates that the image does not employ archive-based or file concatenation steganography techniques. Based on this finding, further investigation should focus on alternative steganographic methods rather than embedded file extraction.

3. Steganographic Data Extraction Using Steghide



```
┌──(kali㉿kali)-[~/Steganography]
└─$ steghide extract -sf Extinction_1577976250757.jpg
Enter passphrase:
wrote extracted data to "Final_message.txt".

┌──(kali㉿kali)-[~/Steganography]
└─$ cat Final_message.txt
It going to be over soon. Sleep my child.

THM{500n3r_0r_l473r_17_15_0ur_7urn}
```

The screenshot shows the use of the steghide tool to extract concealed data from the image **Extinction_1577976250757.jpg**. The command steghide extract -sf Extinction_1577976250757.jpg was executed, where the -sf option specifies the stego file from which hidden data is to be extracted. Upon execution, the tool prompted for a passphrase; however, no passphrase was required for this image, and the extraction was successfully completed by pressing **Enter**. This indicates that the embedded data was not protected by encryption or a password.

As a result of the extraction process, a file named **Final_message.txt** was recovered. Viewing the contents of the extracted file revealed a hidden message followed by a flag: *"It going to be over soon. Sleep my child."* and **THM{500n3r_0r_l473r_17_15_0ur_7urn}**. This confirms that steganography was actively used within the image to conceal textual data and validates the effectiveness of steghide for extracting hidden information from JPEG images.