Mission Name
The truth

Historical Background
In their relentless pursuit of the truth, Ethan and Claire receive a critical piece of evidence from Dr. Pinche. The missing footage from Jailnor's holding room at Skytech could hold the key to understanding his fate. However, the images are in disarray, scrambled beyond immediate recognition. Dr. Pinche, unable to decipher the data, entrusts Ethan with this crucial task.

Technical High-Level Overview
Ethan is faced with a complex challenge: to analyze and reorder the scrambled footage provided by Dr. Pinche. This task requires a keen eye for detail and a deep understanding of image analysis techniques. The secret hidden within these images is vital for unraveling the mystery surrounding Jailnor's circumstances and could potentially expose hidden truths about Skytech.

Short Mission Description
Ethan, the information from Dr. Pinche is now in your hands. Your mission is to sift through the scrambled footage, reassemble the images correctly, and extract the concealed truth about what happened to Jailnor. Your skills in data analysis and decryption are crucial to success. Good luck on your quest for the truth.

Mission Description
Dr. Pinche has managed to obtain the elusive footage from Jailnor's holding room within the confines of Skytech, a piece of the puzzle that has remained missing until now. Unfortunately, the footage is not in a viewable state; the images are jumbled and need to be meticulously reorganized. Unable to solve this puzzle himself, Dr. Pinche turns to Ethan, hoping his expertise can unlock the secrets held within. It's a race against time to piece together the footage and shed light on the events that transpired in Jailnor's holding room.

Location
RECON CAR – AIR

Questions

What is the byte used to hide the password?

- 0

What is the the password discovered to open the zip file?

- U_Have_Discovered_The_Truth

What is the sounds listened in the mp3 file?

- DFTM

Hints

1. Search for hidden text in file discover_the_truth.png
2. The 0-byte is used to hide the password that allow to open the zip file hidden
3. Use DTFM frequencies or auto detect tools to recover the flag

Categories

- Steganography

Write Up

To follow through with the challenge as described in the provided writeup, let's break down the process into detailed steps to uncover the hidden message. This challenge involves multiple stages, including image steganography, password extraction, audio file analysis, and DTMF (Dual-Tone Multi-Frequency) decoding to reveal the final flag.

Step 1: Jpg Content Contains Zip File

The initial clue is that a JPG image contains a hidden ZIP file. Tools or methods to reveal such hidden content could include steganography analysis tools or direct inspection methods.

Step 2: Extracting Password from an Image

The password for the ZIP file is hidden within a 0-bit layer of another image named discover_the_truth.png`. To extract this password, the writeup suggests using a tool available at [Image-Stegano GitHub repository](https://github.com/varunon9/Image-Stegano).

Step 3: Unzipping the File

With the password extracted from the steganographic image, unzip the file to reveal its contents, which is an MP3 file featuring DTMF sounds.

Step 4: Analyzing the MP3 File

To interpret the DTMF sounds within the MP3 file, the writeup suggests using Audacity, a software capable of analyzing audio frequencies, or online autodetection tools like the ones mentioned ([DTMF Detect](https://unframework.github.io/dtmf-detect/), [Zeta Two CTF writeup](https://zeta-two.com/ctf/2015/10/04/sectctf-writeup.html)).

Step 5: Decoding DTMF to Hexadecimal

The DTMF tones translate to a hexadecimal string: `66626167725330756364533173534265683163645374683353747275746873`. This string, when partially decoded, resembles an incomplete flag with missing characters related to hexadecimal values that could represent letters (a-f).

Step 6: Adjusting the Hexadecimal String

By recognizing that the hexadecimal string contains parts of the flag but lacks proper hexadecimal-to-text conversion for some characters, adjustments are made. Inserting the correct hex values for 'a', 'b', 'c', and 'd' where they logically fit within the context of a flag format, the corrected hexadecimal string is obtained: `666c61677b5330756e645f31735f426568316e645f7468335f74727574687d`.

Step 7: Final Decodification

Converting the corrected hexadecimal string to ASCII reveals the hidden message and the final flag: `flag{S0und_1s_Beh1nd_th3_truth}`.

This challenge demonstrates a multifaceted approach to CTF challenges, requiring knowledge across different domains, including steganography, password cracking, audio analysis, and hexadecimal decoding. The ability to piece together clues from various sources and adjust strategies based on partial information is key to uncovering the concealed flag.

Flag Information

flag{S0und_1s_Beh1nd_th3_truth}