Forensics CTF 10

Platform: picoCTF 2019

Challenge Name: m00nwalk2

Category: Forensics

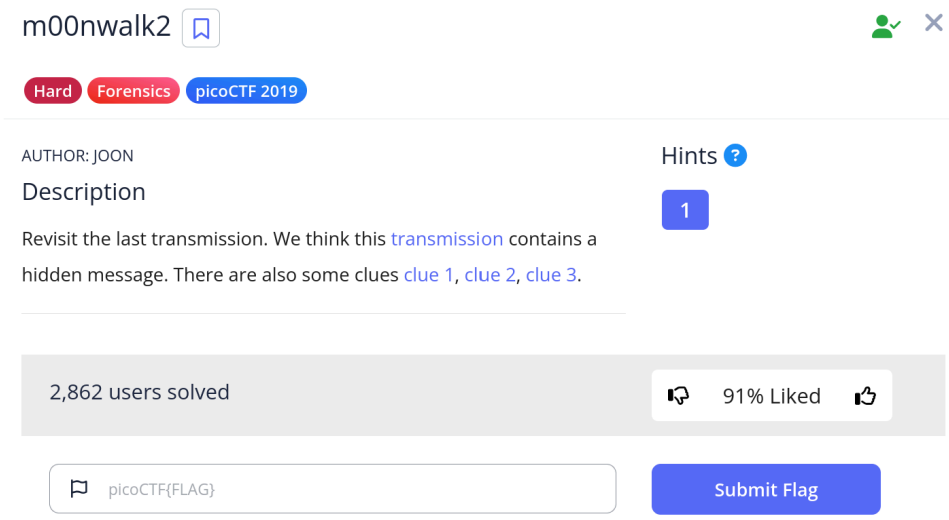
Difficulty: Hard

Submitted By: Gurleen Kaur Brar

Objective

The objective was to extract a hidden message embedded inside an audio file using steganography techniques, guided by visual clues. The challenge built upon prior knowledge and hinted at tools and passwords hidden in plain sight.

Challenge Description



Files and Tools Used

- **Files Provided:**
  - `message.wav`

- `clue1.wav`, `clue2.wav`, `clue3.wav` (clues with SSTV-encoded images)

- **Tools Used:**
  - `qsstv` (to decode visual SSTV transmissions)
  - `steghide` (to extract hidden payload from `.wav`)
  - Kali Linux terminal

```
┌──(gurleen㉿kali)-[~/ctf]
└─$ cd moonwalk

┌──(gurleen㉿kali)-[~/ctf/moonwalk]
└─$ ls
clue1.wav  clue2.wav  clue3.wav  message.wav
```

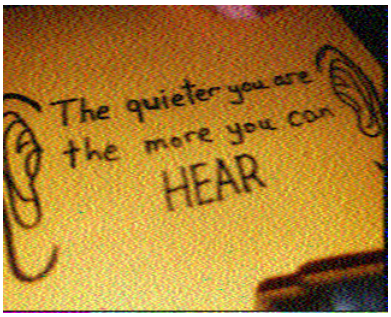
Step-by-Step Process

Step 1: Decode Clue Images with QSSTV

Opened the `.wav` clue files in QSSTV to extract the visual messages. The three decoded images revealed:

1. **Clue 1:** “Password: hidden_stegosaurus”
2. **Clue 2:** “The quieter you are, the more you can HEAR”
3. **Clue 3:** “Alan Eliassen – the Future Boy”

These images served as both the password hint and the steganography theme.



Step 2: Extract Hidden Data from message.wav

Used the password from Clue 1 and extracted the hidden payload from `message.wav` using:

```
steghide extract -sf message.wav -p hidden_stegosaurus
```

This successfully generated `steganopayload12154.txt`.

Step 3: Read the Extracted File

Opened the payload file to reveal the hidden flag:

```
cat steganopayload12154.txt
```

```
┌──(gurleen㉿kali)-[~/ctf/moonwalk]
└─$ steghide extract -sf message.wav -p hidden_stegosaurus
wrote extracted data to "steganopayload12154.txt".

┌──(gurleen㉿kali)-[~/ctf/moonwalk]
└─$ ls
clue1.wav  clue2.wav  clue3.wav  message.wav  steganopayload12154.txt

┌──(gurleen㉿kali)-[~/ctf/moonwalk]
└─$ cat steganopayload12154.txt
picoCTF{the_answer_lies_hidden_in_plain_sight}
```

Flag Submitted

```
picoCTF{the_answer_lies_hidden_in_plain_sight}
```

The flag was extracted correctly and submitted successfully.