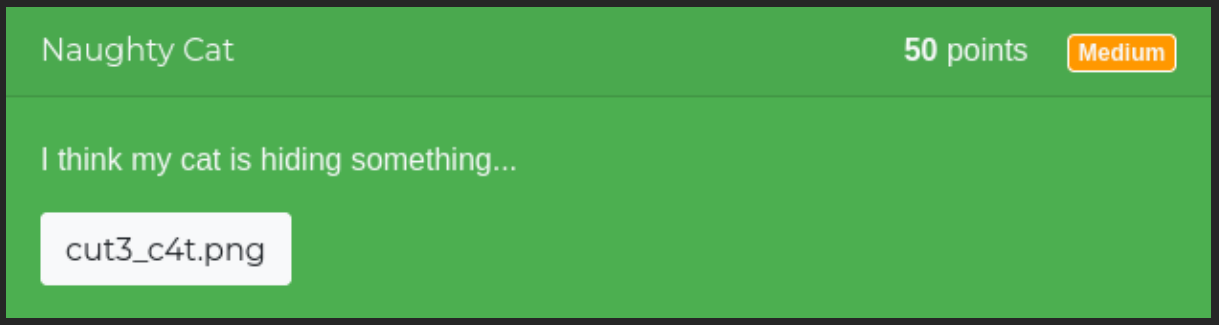
Naughty Cat CTF Writeup

This document is a walkthrough on one way to solve the **Naughty Cat CTF** on **CTFLearn**. The objective is to explain how I was able to solve this CTF to my future self.

General Information

- *Difficulty:* Medium
- *Category:* Forensics
- *Link:* Challenge - Naughty Cat - CTFlearn - CTF Practice

Introduction



We're given a PNG file, which looks like this:

Little did we know, this cat was hiding a profound secret!

Let's start with a simple strings command on the file to see if there's anything hidden:

```
┌──(alexandre㉿vbox)-[~/Pictures]
└─$ strings cut3_c4t.png | tail
@9zg
f2}*
7@:Z
yW<UL
y0u_4r3_cl0s3.rar
Cat!
f1n4lly.txt0
K_Vk
 gY
purrr_2.mp3
```

This result suggests hidden files such as *y0u_4r3_cl0s3.rar*, or *f1n4lly.txt*, are in the image file, so we're going to use a tool called **binwalk** to extract them**.**

```
┌──(alexandre㉿vbox)-[~/Pictures]
└─$ binwalk -e cut3_c4t.png
```

```
┌──(alexandre㉿vbox)-[~/Pictures]
└─$ ls
_cut3_c4t.png-0.extracted  cut3_c4t.png
```

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ ls
28E4B.rar  29  29.zlib  purrr_2.mp3  y0u_4r3_cl0s3.rar
```

Let's do a quick "strings" on *purrr_2.mp3*; it suggests that it's hiding some sort of password.

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ strings purrr_2.mp3 | head
 -TPE1
is a password here?
Xing
!#&'*,/147:<?BEHJLNQSVY\^adgilopsuxz}
PLAME3.99r
<<<z
h@cW
\s>R
I1Sv(
       2#*n
```

Same thing on *y0u_4r3_cl0s3.rar*, it looks like a file is inside.

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ strings y0u_4r3_cl0s3.rar

Cat!
f1n4lly.txt0
K_Vk
```

However, it's not a RAR file, it's a data file; it looks like the file was modified to corruption.

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ unrar x y0u_4r3_cl0s3.rar

UNRAR 7.01 freeware      Copyright (c) 1993-2024 Alexander Roshal

y0u_4r3_cl0s3.rar is not RAR archive
No files to extract

┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ file y0u_4r3_cl0s3.rar
y0u_4r3_cl0s3.rar: data
```

Looking at the file in Hexadecimal form, we see that the file signature is incorrect for a RAR file, so let's change it according to what's stated on [List of file signatures - Wikipedia]

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ xxd y0u_4r3_cl0s3.rar
00000000: 4361 7421 1a07 0100 3392 b5e5 0a01 0506  Cat!....3.......
00000010: 0005 0101 8080 007c bc22 8d58 0203 3c90  .......|."·X··<·
00000020: 0104 c102 2067 b83d 0880 0300 0b66 316e  .... g·=·····f1n
00000030: 346c 6c79 2e74 7874 3001 0003 0f67 c16b  4lly.txt0····g·k
00000040: 5eea ad33 4801 8fe1 06a1 a1b4 9cd8 7130  ^··3H·········q0
00000050: d73e 873b f253 bf05 2444 2af9 7806 4f48  ·>·;·S··$D*·x·OH
00000060: 7a08 9021 dcde 2e38 b30a 0302 7d84 a466  z··!···8····}··f
00000070: 0f01 d601 1485 be3b 2d96 5f8c 4f57 4711  ·······;-·_·OWG·
00000080: b087 2992 f043 d1ee ab9a 4f1a 3408 dc6a  ··)··C····O·4··j
00000090: fd43 2438 9f7c c279 9461 8767 409d 196d  ·C$8·|·y·a·g@··m
000000a0: f2b3 4377 9aa9 f326 ba94 fa90 88e7 e1f3  ··Cw···&········
000000b0: 3f4f ca1b 9ccb 4b5f 566b 915a 0f03 7572  ?O····K_Vk·Z··ur
000000c0: 9c39 4967 f1c7 1499 10b4 78cf 6cbb eae9  ·9Ig·····x·l···
000000d0: 9035 eb88 bcff 9ae3 2d2e eab2 2cdc c281  ·5·····-···,···
000000e0: 8fde 1db7 a8ab ea0d 8863 8e80 0ee3 1c37  ·········c·····7
000000f0: 9205 0565 28b2 cb2b d9fb 67d0 6263 bbe7  ···e(··+··g·bc··
00000100: be57 694a 1d77 5651 0305 0400            ·WiJ·wVQ····
```

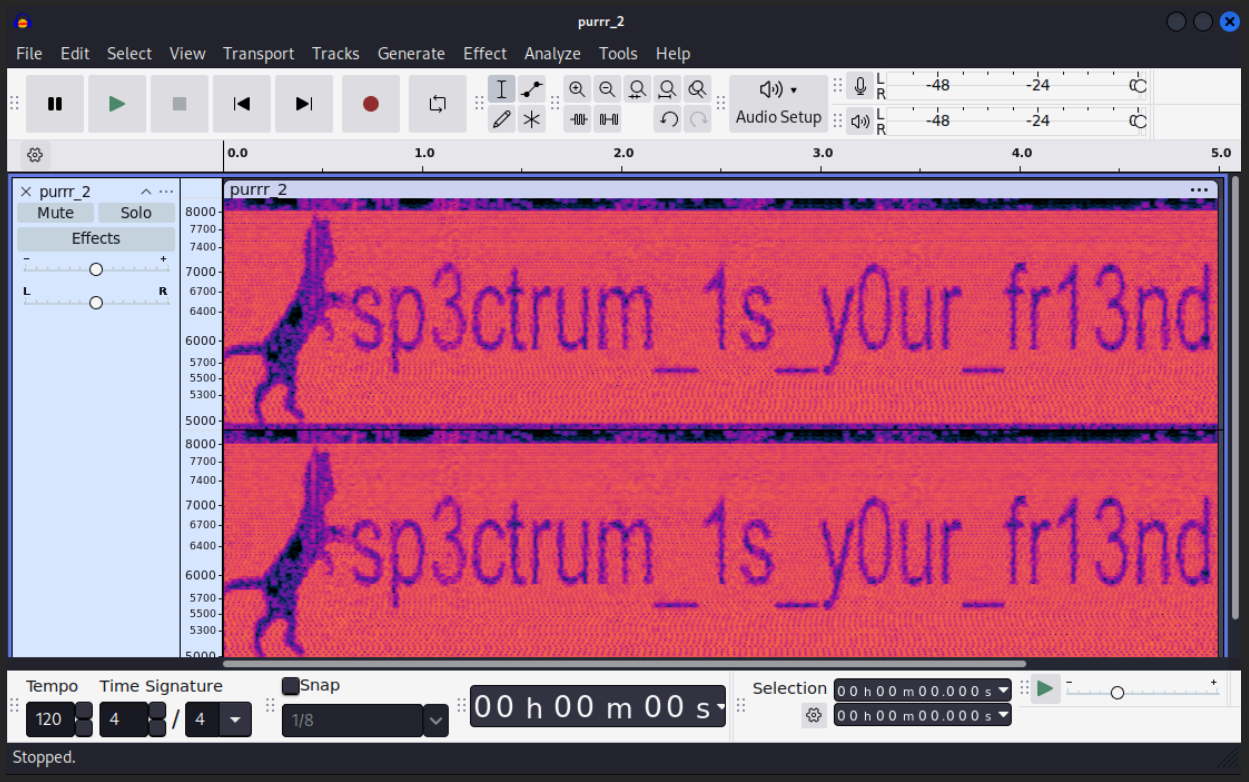
52 61 72 21 1A 07 01 00	Rar! SUBBELSOHNUL	0	rar	Roshal ARchive compressed archive v5.00 onwards[24]

It's meant to be "52 61 72 21 1A 07 01 00", not "43 61 74 21 1A 07 01 00"

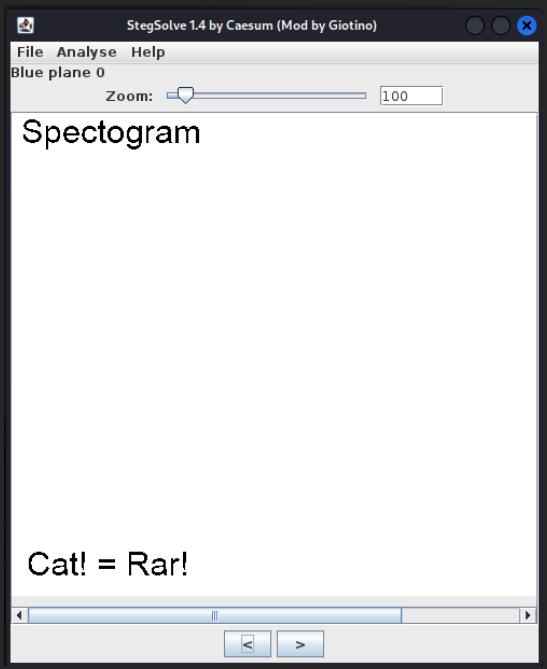
Using hexedit to modify the hexadecimal value of the file signature, we're capable of extracting the RAR file, but it asks us for a password, so we'll need to take a closer look at the *purrr_2.mp3* file.

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ unrar x y0u_4r3_cl0s3.rar

UNRAR 7.01 freeware      Copyright (c) 1993-2024 Alexander Roshal

Extracting from y0u_4r3_cl0s3.rar

Enter password (will not be echoed) for f1n4lly.txt:
```

Purrr_2.mp3 is an mp3 file, and the password is probably hidden in there. A logical thing to try is doing a spectrographic analysis on the file.
Using Audacity, an audio-editing software, we see that there's effectively a hidden message: ***"sp3ctrum_1s_y0ur_fr13nd"***



Note: Using a tool called stegsolve, there was also a clue towards this being hidden in plain sight, which is revealed by taking a specific bit plane of the image.



And that’s the password.

```
Extracting from y0u_4r3_cl0s3.rar

Enter password (will not be echoed) for f1n4lly.txt:

Extracting  f1n4lly.txt
All OK
```

We can then extract a text file *f1n4lly.txt* from it, and it gives us the flag in base64 format

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ strings f1n4lly.txt
          __/|
          \o.O|
        _____(___)_____
       |       U       |________    __
       |ZjByM241MWNzX21h|        |__|  |_________
       |________________|NXQzcg==| ::|  |         /
       |                 \._______|::|__|        <
       |                          \::/  \._______\
       |
       |
```

```
┌──(alexandre㉿vbox)-[~/Pictures/_cut3_c4t.png-0.extracted]
└─$ echo 'ZjByM241MWNzX21hNXQzcg==' | base64 -d
f0r3n51cs_ma5t3r
```

f0r3n51cs_ma5t3r